



Retouradres: Postbus 93122, 2509 AC Den Haag



Geachte 

Op 16 juli 2025 heeft u de Nationale ombudsman gevraagd om openbaarmaking van informatie die de Nationale ombudsman onder zich heeft op het gebied van AVG-compliance in de periode van 2018 tot heden. U verstaat hieronder AVG-implementatiedocumenten, de in deze periode gemaakte impactanalyses voor de gegevensverwerking (PIA/DPIA), AVG-impactanalyses bij aanbestedingen, algemeen AVG-beleid ten aanzien van gegevens van medewerkers en andere betrokkenen. Uw verzoek wordt aangemerkt als verzoek om openbaarmaking op grond van artikel 4.1 van de Wet open overheid (Woo).

Verduidelijking van verzoek

Naar aanleiding van het gesprek om verduidelijking van uw verzoek is het verzoek gespecificeerd tot de volgende onderwerpen:

- Personeelsbeleid
- Ontwikkeling van de AVG binnen de ombudsman vanaf 2018 (beleid door de jaren heen)
- Implementatie van de AVG (incl. concepten)
- DPIA's
- Aanbestedingsprocedures (gericht op bescherming van persoonsgegevens)
- Handleiding AVG-verzoek
- Handleiding melden datalek
- Hoe omgaan met gegevens van burgers bij No
- Adviesrol van de ombudsman bij consultatie wetgeving

Mijn besluit

Met de door u aangegeven zoektermen: AVG- Algemene Verordening Gegevensbescherming - privacy - privacyrisico - wetgevingstoets - PIA - Privacy Impact Assessment - gegevensbeschermingseffectbeoordeling - privacyeffectbeoordeling - DPIA - Data Protection Impact Assessment - FG - Functionaris Gegevensbescherming - datalek - gegevensbescherming - persoonsgegevens - bijzondere persoonsgegevens - AP - Autoriteit Persoonsgegevens, is er gezocht in ons zaak- en archiefsysteem en mailboxen.

Bij deze zoekslag zijn 43 documenten aangetroffen. Deze documenten zijn benoemd in de inventarislijst.

In deze lijst zijn eveneens de documenten opgenomen die al openbaar zijn. De verwijzing naar de vindplaats is opgenomen in de inventarislijst.

Pagina 1

Datum

5 september 2025

Onderwerp

Woo-besluit AVG-compliance

Ons nummer

2271381

Uw kenmerk

Bijlage(n)

Contactpersoon



Nationale ombudsman

Bezuidenhoutseweg 151
2594 AG Den Haag

Postbus 93122
2509 AC Den Haag

T 070 356 35 63
post@nationaleombudsman.nl
www.nationaleombudsman.nl



Waarom in sommige documenten gegevens niet leesbaar zijn

De documenten moet ik beoordelen op grond van artikel 5.1, eerste, tweede of vijfde lid, of artikel 5.2, eerste lid, van de Woo. In deze artikelen staat welke gegevens niet mogen worden verstrekt.

In de inventarislijst is aangegeven welke uitzonderingsgrond van toepassing is geweest bij het weglakken van informatie.

Pagina 2

Ons nummer

2271381

Informatie die met de aanduiding 'J' onleesbaar is gemaakt

Op grond van artikel 5.1, tweede lid, aanhef en onder e, kan ik geen informatie openbaar maken als dit de persoonlijke levenssfeer schaadt en dit belang zwaarder weegt dan het belang van openbaarheid. Het gaat om persoonsgegevens die (indirect) te herleiden zijn tot een persoon, zoals namen, e-mailadressen, telefoonnummers en functienamen. Ik vind het in dit geval belangrijk dat de identiteit van mijn medewerkers en van betrokkenen niet bekend wordt omdat dit zijn of haar privacy kan schenden. Dat vind ik niet wenselijk. Daarom maak ik deze persoonsgegevens niet openbaar.

Informatie die wel is benoemd maar waarvan de documenten niet zijn toegevoegd

Op grond van artikel 5.2, eerste lid, worden persoonlijke beleidsopvattingen in documenten die bestemd zijn voor intern beraad niet openbaar gemaakt. Persoonlijke beleidsopvattingen zijn (ambtelijke) adviezen, meningen, visies, standpunten en overwegingen ten behoeve van intern beraad. Wat niet onder persoonlijke beleidsopvattingen valt, zijn feiten, prognoses, beleidsalternatieven, de gevolgen van een bepaald beleidsalternatief of andere onderdelen met een overwegend objectief karakter. Het is van belang dat ambtenaren intern vrij met elkaar van gedachten moeten kunnen wisselen over beleidskeuzes. Een zekere mate van veiligheid is nodig om te kunnen komen tot een effectieve besluitvorming. Gelet hierop worden de documenten met de titel 'document 1628385' en 'document 1641105' in het geheel niet openbaar gemaakt. Dit betreft communicatie tussen de Nationale ombudsman en de Ondernemingsraad aangaande de aanstelling van de Functionaris Gegevensbescherming. Eveneens worden de documenten met de titel 'Protocol datalekken V1.1' en 'Beleid DPIA-scan v0.6 0410202' in zijn geheel niet openbaar gemaakt. Deze informatie is nog niet definitief vastgesteld en is derhalve onderdeel van het interne beraad.

Informatie die met de aanduiding 'K' onleesbaar is gemaakt

In het document met de titel 'DPIA-Datamask applicatie v1.0' is informatie met de aanduiding 'K' onleesbaar gemaakt.

Op grond van artikel 5.1, tweede lid aanhef en onder f kan ik geen informatie openbaar maken over concurrentiegevoelige bedrijfs- en fabricagegegevens. Ik ben van mening dat het belang van deze derde-belanghebbende zwaarder weegt dan het belang van openbaarmaking. Het document bevat bedrijfsgevoelige en beveiligingskritische informatie. Deze informatie kan zowel mijn organisatie als de derde-belanghebbende schaden. Daarom maak ik deze informatie niet openbaar.

Informatie die met de aanduiding 'T' onleesbaar is gemaakt

In document met de titel 'personeelshandboek -14' is informatie met de aanduiding 'T' onleesbaar gemaakt. Deze informatie heeft geen betrekking op de door u gevraagde bestuurlijke aangelegenheid (AVG-compliance) en valt daarom buiten de reikwijdte van de Woo.



De Woo ziet niet op het genereren van documenten

De Woo heeft betrekking op openbaarmaking van informatie die neergelegd is in documenten. Alleen bestaande documenten vallen onder de Woo; als documenten niet bestaan, kan ik deze niet openbaar maken en hoef ik deze ook niet te genereren.

De Nationale ombudsman maakt gebruik van de GRCControl-tool om grip te houden op Informatiebeveiliging en Privacy Management. Alle processen en producten in gebruik door de Nationale ombudsman zijn ondergebracht in deze tool en worden door middel van een PDCA cyclus getoetst op de BIO-normering en de AVG.

Pre-DPIA's en DPIA's worden ook uitgevoerd in deze tool. Het is echter niet mogelijk om informatie in documentvorm te genereren uit deze tool.

Zienswijze van derden

Omdat uw verzoek mede betrekking heeft op een derde-belanghebbende, heb ik deze persoon om zijn zienswijze gevraagd. De zienswijze is verwerkt in dit besluit.

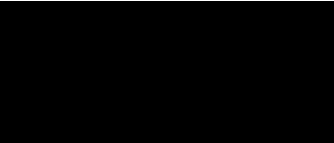
Wijze van bekendmaking

Naast dat het besluit aan u wordt toegezonden, zullen het (geanonimiseerde) besluit en de bijbehorende documenten worden gepubliceerd op onze website.

Vragen

Als u vragen heeft over de afhandeling van uw verzoek, dan kunt u contact opnemen met de Woo-coördinator. U kunt haar bereiken via telefoonnummer (070) [REDACTED]. Mailen naar woo@nationaleombudsman.nl kan ook. Denk er dan aan om uw dossiernummer (2271381) te vermelden.

Met vriendelijke groet,
namens de Nationale ombudsman,



Hanneke van Essen
Algemeen directeur





Bezwaar

Bent u het niet eens met deze reactie? Neem dan gerust contact met ons op. Doe dit wel ruim binnen de bezwaartermijn van zes weken.

Komt u er daarna nog niet uit? Dan kunt u binnen zes weken na de datum van verzending van het besluit een bezwaarschrift indienen.

Het bezwaarschrift bevat de volgende informatie:

- uw naam en adres;
- de datum waarop u het bezwaarschrift schrijft;
- een omschrijving van het besluit waar u het niet mee eens bent en het bijbehorende dossiernummer;
- de reden van uw bezwaar;
- uw handtekening.

Een bezwaarschrift kunt u indienen via de mail (jz@nationaleombudsman.nl) of per post (Nationale ombudsman, Postbus 93122, 2509 AC Den Haag).

Aan het indienen van een bezwaarschrift zijn geen kosten verbonden. Als er naast u nog andere belanghebbenden betrokken zijn bij dit besluit, dan kunnen zij ook bezwaar maken tegen het besluit.

Voorlopige voorziening

Het indienen van een bezwaarschrift schort de werking van het besluit niet op. Dat betekent dat het besluit blijft gelden in de tijd dat uw bezwaarschrift in behandeling is. Meent u dat de betrokken belangen zo zwaar wegen dat u de beslissing op uw bezwaar niet kunt afwachten? Dan kunt u tegelijkertijd met of na indiening van uw bezwaarschrift een verzoek om voorlopige voorziening indienen bij de rechtbank. Hiervoor betaalt u griffiekosten. U kunt ook digitaal een verzoekschrift indienen bij deze rechtbank via <https://loket.rechtspraak.nl/bestuursrecht>. Daarvoor moet u wel beschikken over een elektronische handtekening (DigiD). Kijk ook op de genoemde website voor de precieze voorwaarden.

INVENTARISLIJST BEHORENDE BIJ WOO-BESLUIT 2271381

		Woo artikel/openbaar
1	DPIA- Datamask applicatie v1.0	5.1-2f, 5.1-2h
2	Public+DPIA+Teams+OneDrive+SharePoint+and+Azure+AD +16+Feb+2022	https://open.overheid.nl/details/ronl-06f045ed745d9540ec4262a6079e8e73ad262a43
3	Samenvatting-NL-DPIA-Teams-OneDrive-Sharepoint-16-Feb-2022	https://slmmicrosoftrijk.nl/wp-content/uploads/2022/02/Samenvatting-NL-DPIA-Teams-OneDrive-Sharepoint-16-Feb-2022.pdf
4	Adviezen PIA v02	-
5	Document - 1616385	5.1-2e
6	Document - 1617130	5.1-2e
7	Document - 1617132	5.1-2e
8	Document - 1623437	5.1-2e
9	Document - 1624766 1661044	-
10	Document - 1628385	5.2-1
11	Document - 1635026 1661556	-
12	Document – 1641105	5.2-1
13	Document - 1641764 1661817	5.1-2e
14	Document - 1646646	-
15	Document - 1650985	5.1-2e
16	Document - 1656924 1662316	-
17	Document - 1659727 1662376	-
18	Document - 1672299 1662780	5.1-2e
19	PIA Junni 2018 en rapport status implementatie AVG	-
20	20210917 Incident_Management_v1.0	5.1-2e
21	20220523 Leeg Formulier Wijzigingsbeheer_v2.1	-
22	20220603 Wijzigingsbeheer_v2.2	5.1-2e
23	Beleid DPIA-scan v0.6 04102024 concept	5.2-1
24	beleid-bescherming-persoonsgegevens	-
25	Bijlage Informatiebeveiliging en Privacy bij Leveranciersrelaties - Ombudsman V1.1	-
26	Formulier datalek	Website Nationale ombudsman (Woo- besluiten, 2024 nr 3)
27	Informatiebeveiliging en Privacy Bewustzijn Beleid 2024-2026 v1.0.1 DEFINITIEF	5.1-2e
28	Informatiebeveiliging en Privacy bij Leveranciersrelaties - Ombudsman v1.0 DEFINITIEF	5.1-2e
29	Informatiebeveiliging en Privacy Governancebeleid 2025- 2028	5.1-2e
30	informatieblad interne medewerkers	-
31	Leeg Formulier pre-DPIA scan v09	-

32	model-verwerkersovereenkomst-arbit-2022-feb2024	Algemene Rijksinkoopvoorwaar den bij IT-overeenkomsten (ARBIT) PIANOo - Expertisecentrum Aanbesteden
33	Operationele uitvoering AVG verzoeken v0.10 16112020	-
34	Privacy beleid Nationale ombudsman v1.0	Website Nationale ombudsman (Woo- besluiten, 2025 nr 5)
35	Privacy by design_v0.4 20082021 AEK	5.1-2e
36	Privacy verklaring website 2024 def	Website Nationale ombudsman
37	Procesbeschrijving AVG-verzoeken 2025	-
38	Procesbeschrijving rechten van betrokkene AVG concept	-
39	protocol datalekken No V1.0	Website Nationale ombudsman (Woo- besluiten, 2024 nr 3)
40	Protocol datalekken V1.1	5.2-1
41	Standaardbrieven datalekken	Website Nationale ombudsman (Woo- besluiten, 2024 nr 3)
42	verwerkersovereenkomst-arvodi-2025-maart2025	Algemene Rijksinkoopvoorwaar den voor diensten (ARVODI) PIANOo - Expertisecentrum Aanbesteden
43	personeelshandboek-14	5.1-2e, buiten reikwijdte



Gegevensbeschermingseffectbeoordeling (DPIA)

Naam DPIA: Gebruik van DataMask door de Nationale ombudsman

Uitvoerdatum: 16 september 2024

Aanwezigen: privacy officer & FG



Inhoudsopgave

Inleiding

3

A. 4

1. 4
2. 4
3. 5
4. 5
5. 5
6. 5
7. 6
8. 6
9. 8
10. 8

B. 10

11. 10
12. 10
13. 10
14. 11
15. 11

C. 12

betrokkenen

12

16. 12
17. 14

Instructie:

Dit inhoud van deze DPIA is geaggregeerd op basis van de input die is verkregen vanuit enkele DataMask klanten, waaronder gemeenten, waterschappen en omgevingsdiensten. Deze DPIA kan dienen als model voor de eigen uitvoering door uw organisatie.

De opzet van deze DPIA is gebaseerd op het Rijksmodel DPIA.

De DPIA betreft de applicatie DataMask en ziet uitdrukkelijk niet op het hele proces van verzamelen van documenten uit verschillende systemen, aanbieden aan DataMask en publiceren van documenten via verschillende daarvoor geschikte kanalen.

Vervang letterlijk: de Nationale ombudsman voor de naam van uw organisatie om gemakkelijk de DPIA op uw organisatie toe te passen.

Inleiding

Per 1 mei 2022 is de Wet Open Overheid (WOO) in werking getreden. Deze wet vervangt de Wet Openbaarheid van Bestuur (WOB). Per 1 januari 2023 zal ook de Wet Elektronische Publicaties (WEP) volledig in werking treden.

Deze twee wetten verplichten de gemeente om, naast het actief openbaar maken van de vergunningen en beleidsregels, ook informatie die tot een besluit heeft geleid actief openbaar te maken. Dit nog naast de reeds bestaande verplichtingen rondom openbaarmaking op verzoek. De komende jaren komen er steeds meer terreinen bij, waarvan de informatie actief openbaar gemaakt moet worden. In deze informatie wordt veel en vaak privacygevoelige informatie gebruikt en daarbij is het van belang, dat deze wordt geanonimiseerd.

Het manueel anonimiseren van gegevens is een tijdrovende klus waarbij ook veelvuldig fouten optreden en datalekken zijn voorgekomen. Om die reden heeft de Nationale ombudsman ervoor gekozen om anonimiseringssoftware aan te schaffen, genaamd DataMask. Voor het gebruik van de software moeten risico's worden beoordeeld. Wanneer de risico's bekend zijn, kunnen eventuele noodzakelijke beveiligingsmaatregelen worden getroffen om geconstateerde risico's te beperken.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de DPIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Het voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Antwoord:

De Nationale ombudsman is voornemens om met ingang van medio 2022 gebruik te maken van nieuwe software genaamd DataMask om zo documenten (*indien van toepassing* via koppeling met Djuma) te anonimiseren. Door het gebruik van de software van DataMask wordt het risico op datalekken door onzorgvuldig anonimiseren geminimaliseerd en de toenemende hoeveelheid openbaar te maken documenten beheersbaar.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

Antwoord:

De categorie van persoonsgegevens die worden verwerkt door de DataMask applicatie is volledig afhankelijk van het aan DataMask aangeboden document. Dit kunnen dus alle soorten persoonsgegevens zijn, afhankelijk van de publicatieverplichting of -doel waarvoor de oplossing wordt gebruikt. Normaal gesproken gaat het om de volgende persoonsgegevens:

- NAW-gegevens
- Contactgegevens (e-mailadres, telefoonnummer)
- Handtekeningen en parafen
- Financiële gegevens (leges, IBAN, andere kosten)
- Inhoud die zaaktype-gerelateerd is.

Het kan voorkomen dat bijzondere en gevoelige persoonsgegevens worden verwerkt. Dat is afhankelijk van het zaaktype. Er kunnen dus theoretisch de volgende bijzondere/ gevoelige persoonsgegevens worden verwerkt:

- Gegevens over de gezondheid;
- Gegevens waaruit ras of etnische afkomst blijken;
- Gegevens waaruit politieke opvattingen blijken;
- Gegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- Gegevens waaruit het lidmaatschap van een vakbond blijken;
- Gegevens met betrekking tot iemands seksueel gedrag of voorkeur;
- Strafrechtelijke gegevens;
- Het BSN.

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Antwoord:

Het in het kader van wettelijke publicatieverplichtingen, zoals de Wet elektronische publicaties of de Wet open overheid, waaronder de passieve en actieve openbaarmaking, controleren van documenten op persoonsgegevens en/of gevoelige informatie. De controle van de software zorgt voor een verwerking van persoonsgegevens op de servers van DataMask, die worden ingezet voor de verwerkingsdoeleinden zoals hieronder genoemd.

Het opnemen van bepaalde (persoons)gegevens op een automatisch te markeren of automatisch niet te markeren lijst, zodat deze altijd wel of juist nooit worden voorgesteld om te anonimiseren.

Het loggen van het gebruik van de applicatie door gebruikers van de Nationale ombudsman, waarbij wordt vastgelegd wanneer deze door welke gebruiker wordt benaderd.

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Antwoord:

Het via intelligente software geautomatiseerd op zoek gaan naar gegevens, zodat deze datalekken door menselijke fouten kan voorkomen, waarna deze definitief worden verwijderd alvorens tot inzage of openbaarmaking van die documenten kan worden overgegaan.

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Antwoord:

Verwerkingsverantwoordelijke: De Nationale ombudsman (toegang/autorisatie is gelijk aan de toegang tot de originele documenten)

Verwerker: DataMask B.V. (alleen de CTO heeft toegang)



Ontvangers: geen directe ontvangers middels de verwerking anders dan de medewerkers van de verwerkingsverantwoordelijke.

Verstrekker: geen

6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Antwoord:

Verwerkingsverantwoordelijke: voldoen aan wetgeving ter voorkoming van boetes en reputatieschade. De toegenomen druk op de organisatie om meer te publiceren het hoofd te bieden door handmatige taken daarbij te automatiseren

Werknemers: efficiënt en gebruiksvriendelijk persoonsgegevens en andere gevoelige gegevens in documenten weglakken.

Natuurlijke personen en organisaties/ instellingen: effectieve bescherming van de persoonlijke levenssfeer of andere belangen.

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.



8. Techniek en methode van gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-) geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.



Beschrijving van het proces:





Technische details:



Andere technieken:



9. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

Antwoord:

Naast de AVG is de volgende wetgeving van belang:

- Wet open overheid
- Wet elektronische publicaties
- Wet kenbaarheid publiek rechtelijke beperkingen
- Archiefwet

De volgende beleidsstukken zijn van belang:

- Privacybeleid

De volgende norm is van toepassing:

- ISO27001
- Baseline Informatiebeveiliging Overheid (BIO)

10. Bewaartermijnen

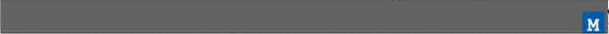
Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Antwoord:

In de cloud-variant van de DataMask applicatie wordt bij het opsturen van een nieuw document naar DataMask (de initiatie van het anonimiseringsproces door een medewerker van de Nationale ombudsman automatisch een geldigheidsdatum bij het document opgeslagen. Dit wordt de initiële bewaartermijn genoemd.  

  maar kan per DataMask-klantomgeving specifiek worden bepaald.

Binnen de initiële bewaartermijn krijgt de gebruiker de kans het document te bewerken in de DataMask-omgeving en worden daarin aangebrachte handelingen (het plaatsen van maskeringen/vlakken), gedurende de initiële bewaartermijn opgeslagen. Na afloop van de initiële bewaartermijn wordt het document definitief verwijderd van DataMask-server, waarna deze dien ten gevolge niet meer aan te roepen is voor de gebruiker. Niet afgeronde documenten zullen opnieuw moeten worden geanonimiseerd.

Zodra een document wordt afgerond of geannuleerd, wijzigt de status en wordt een nieuwe geldigheidsdatum aan het document toegekend, dit wordt de uiterlijke bewaartermijn genoemd.  . Deze termijn dient als enig doel de gebruiker de mogelijkheid te bieden om het geanonimiseerde bestand te kunnen downloaden naar de eigen omgeving, na afronding van het anonimiseren. Na afloop van de uiterlijke bewaartermijn is het geanonimiseerde document niet meer beschikbaar op de DataMask-server. Niet gedownloade documenten zullen opnieuw moeten worden geanonimiseerd.

In een gekoppelde situatie met een zaakstelsel of DMS kan de uiterlijke bewaartermijn korter worden ingesteld omdat bij het afronden van het proces er geautomatiseerd voor wordt gezorgd dat de documenten worden terugschreven naar de specifieke zaak waar vanuit het origineel aan DataMask werd aangeboden.

Op de achtergrond draait een proces op de DataMask-server dat monitort of er documenten verlopen zijn en, zo ja, zorgt dat deze worden verwijderd. Het beleid is onderdeel van de standaard DataMask-software, via de volgende broncode:



Documenten worden niet in een back-up opgeslagen.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de DPIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Antwoord:

De verwerking van persoonsgegevens op grond van de volgende rechtsgronden is mogelijk:

- de gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- de gegevensverwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

De grondslag die hier van toepassing is betreft het voldoen aan een wettelijke verplichting.

12. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

Antwoord:

(bijzondere) Persoonsgegevens die voorkomen in de documenten die aan het verwerkingsmiddel worden toegekend worden verwerkt in de zin van (tijdelijke) opslag op de serveromgeving van de Nationale ombudsman binnen de DataMask omgeving. Het is niet vooraf eenduidig te definiëren welke gegevens dit zullen zijn – aangezien dit afhankelijk is van de documenten die aan DataMask door gebruikers van de Nationale ombudsman worden toegevoegd, maar deze kunnen in uitzonderlijke gevallen ook bijzondere persoonsgegevens bevatten. De software maakt het mogelijk om deze gegevens eenvoudig te vinden in documenten zodat ongeoorloofde verstrekking (die uitmonden in datalekken), bijvoorbeeld in het kader van een Woo-verzoek, kan worden voorkomen. Het BSN-nummer wordt door de software geïdentificeerd op basis van het patroon (reguliere expressie), en aan gebruikers gesuggereerd. Deze gegevens worden niet verder opgeslagen, behalve in de (tijdelijke) opslag van het document t.b.v. het anonimiseren van deze gegevens.

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Antwoord:

Door het verwerkingsmiddel en de organisatie DataMask worden gegevens niet voor een ander doel verwerkt dan het tijdelijk opslaan van deze documenten ten behoeve van het anonimiseren van de (persoons)gegevens door gebruikers van de Nationale ombudsman. Verwerkte of aangemerkte gegevens worden niet opgeslagen in een database, enkel worden daarvan de x/y-posities opgeslagen. De verdere ontwikkeling en training van de intelligente technieken vindt separaat plaats en niet op basis van de door de Nationale ombudsman toegevoegde documenten. Dit maakt dat aan het vereiste van doelbinding wordt voldaan.

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

- Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

1.

Antwoord:

De voorgenomen verwerking zorgt bij uitstek voor bescherming van de persoonlijke levenssfeer doordat het risico op ongeoorloofde verstrekking, zoals bij handmatig anonimiseren veel in de praktijk is voorgekomen, dankzij intelligentie technieken afneemt. DataMask garandeert zelfs contractueel dat de geanonimiseerde gegevens voor 100% definitief uit de documenten worden verwijderd. De noodzaak voor het gebruik van een intelligentie oplossing voor anonimiseren van (persoons)gegevens is groot, nu het aantal publicatieverplichtingen toeneemt, bijvoorbeeld onder de Wet open overheid. Doordat de bewaar- en vernietigingstermijnen zijn te bepalen is de verwerking proportioneel, de tijdelijke verwerking voorkomt mogelijke definitieve gevolgen in het kader van een datalek. Aan de subsidiariteit wordt voldaan omdat de handmatige verwerking (het alternatief voor dit verwerkingsmiddel) geen optie meer is gebleken, gezien het toegenomen aantal documenten dat moeten worden geanonimiseerd.

15. Rechten van de betrokkene

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

Antwoord:

Bij de Nationale ombudsman bestaat er een procedure voor de uitvoering van rechten van betrokkenen. Daarin staat beschreven op welke manier verzoeken worden afgehandeld binnen de Nationale ombudsman. Ook in de privacyverklaring van de Nationale ombudsman(website) staan de rechten van betrokkenen benoemd. In de privacyverklaring staat vermeld op welke manier en waar betrokkenen hun rechten onder de AVG kunnen uitoefenen. Indien hulp voor de uitvoering van een van de AVG-rechten is vereist vanuit de verwerker dan werkt deze daaraan mee, ingevolge de afspraken in de verwerkersovereenkomst.

Voor wat betreft het gebruik van de AI-module van DataMask biedt de "Verklaring omtrent AI", verstrekt door DataMask, de benodigde transparantie en inzicht in deze specifieke verwerking.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
- de oorsprong van deze gevolgen;
- de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.



Wat is de waarschijnlijkheid van het risico?





D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de DPIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Antwoord:



Na bovenstaande maatregelen zijn restrisico's beheersbaar en acceptabel. Een en ander moet ook worden gezien in het licht van de momenteel gelopen risico's bij het anonimiseren van documenten, waar bij de start van de voorgenomen verwerking substantiële winst is te halen op zowel het organisatorisch als technische vlak.



Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

K Art. 5.1 lid 2 sub f

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van de bescherming van andere dan in art. 5.1 lid 1 sub c genoemde concurrentiegevoelige bedrijfs- en fabricagegegevens

M Art. 5.1 lid 2 sub h

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van de beveiliging van personen en bedrijven en het voorkomen van sabotage



Adviesrapport

Adviezen n.a.v. PLA juni 2018

1	Versiebeheer	3
2	Inleiding	4
3	Adviezen	5
3.1	Primair Proces	5
3.1.1	P.1 Toegankelijkheid klachten binnen Verseon.	5
3.1.2	P.2 Opschoonprocedure voor dossiers in Verseon	5
3.1.3	P.4 Gegevens buitenwettelijke klachten worden te lang bewaard	5
3.1.4	P.5 Gedeelde NAW gegevens tussen KOM en No.....	5
3.1.5	P.6 Het online anoniem indienen van een klacht verdwijnt.	6
3.1.6	P.8 Gebruik persoonsgegevens voor structurele aanpak (SA) heeft een ander doel	6
3.1.7	P.11 informatiedeling met organisaties	7
3.1.8	P.12 zichtbaarheid VIP lijst.....	7
3.1.9	P.13 Via NoHow zijn klachtendossiers te zoeken en in te zien	7
3.1.10	P.14 Interne uitwisseling dossierinformatie kan leiden tot datalekken.....	8
3.2	Medewerkers	8
3.2.1	M.4 Informatie omtrent re-integratie wordt te lang bewaard	8
3.2.2	M.8 Medewerkers zijn niet goed op de hoogte van rechten en opslag van eigen persoonsgegevens.....	8
4	Uitgevoerde adviezen.....	10
4.1.1	P.3. Er worden meer persoonsgegevens verzameld en opgeslagen dan strikt noodzakelijk	10
4.1.2	P.9 Gebruik privé-toestel verhoogd kans op datalekken	10
4.1.3	P.15 Dossierinformatie wordt extern gedeeld via e-mail	10
4.1.4	M.5 Vrijgeven privé adressen	11

1 Versiebeheer

Datum	Versie	Auteur	Aanpassingen
21-9-2018	0.1	██████	
16-10-2018	0.2	██████	Diverse aanpassingen na review

2 Inleiding

In mei 2018 zijn twee Privacy Impact Assessment (PIA) sessies gehouden. Hierbij is één sessie gewijd aan het primaire proces en één sessie aan processen die onder het bestuursbureau vallen.

De resultaten van deze twee sessies zijn samengevat in het document 'Privacy Impact Assessment (PIA)'.

In dat document staat beschreven welke verwerkingen zijn behandeld en worden de risico's van deze verwerkingen toegelicht.

Aan het einde van het document worden een aantal adviezen gedaan om de risico's te minimaliseren.

In dit adviesrapport worden de belangrijkste adviezen die nog niet zijn opgevolgd verder in detail uitgewerkt.

3 Adviezen

3.1 Primair Proces

3.1.1 P.1 Toegankelijkheid klachten binnen Verseon.

Prioriteit	Hoog
Eigenaar	

Klachten in Verseon zijn breed toegankelijk. Hierdoor is de kans op onrechtmatige verwerking (inzien) door iemand die niet rechtstreeks bij de klacht betrokken is aanzienlijk.

Onderzoekers kunnen nu klachten van andere teams inzien en gegevens van alle verzoekers inzien.

Advies:

Op dit moment is FT bezig met het in kaart brengen van de autorisatie wensen en mogelijkheden in Verseon. De resultaten van het onderzoek moeten worden voorgelegd in het ???

3.1.2 P.2 Opschoonprocedure voor dossiers in Verseon

Prioriteit	Midden
Eigenaar	

Er is geen opschoonprocedure voor dossiers in Verseon. Gegevens worden langer bewaard dan noodzakelijk. Risico op onrechtmatig verwerken en grotere impact bij evt. datalekken.

Advies:

Voor alle dossiers die niet naar het Nationaal archief worden overgedragen geldt nu een bewaartermijn van 5 jaar. Dit geldt dus ook voor buitenwettelijke zaken. Er dient onderzocht te worden of deze standaard bewaartermijn van 5 jaar teruggebracht kan worden naar bijvoorbeeld een jaar. Na die periode moet de inhoud van dossiers vernietigd worden.

3.1.3 P.4 Gegevens buitenwettelijke klachten worden te lang bewaard

Prioriteit	Midden
Eigenaar	

Alle klachten worden minimaal 5 jaar bewaard. Dit geldt ook voor buitenwettelijke klachten.

Advies:

Voer een onderzoek uit naar passende bewaartermijnen en pas dit aan in het selectiedocument. Zie ook P2.

3.1.4 P.5 Gedeelde NAW gegevens tussen KOM en No.

Prioriteit	Midden
Eigenaar	

Hierdoor kunnen de verkeerde of onjuiste gegevens worden gebruikt voor contact met de klager, waardoor informatie over klachten naar de verkeerde persoon gaat. Een ander probleem met de NAW gegevens is dat ze niet altijd actueel zijn. Hierdoor komt het voor dat een poststuk naar een oud adres wordt verstuurd.

Advies:

Hier zijn twee scenario's denkbaar die het onderzoeken waard zijn:

Scenario 1: Meer discipline bij onderhoud contactgegevens

Zowel bij FD als bij de onderzoekers kan gestuurd worden op meer discipline bij het up to date houden van contactgegevens van verzoekers. Bij het inboeken van nieuwe klachten en volgstukken moet FD kijken of alle aangeleverde contactgegevens overeenkomen met de gegevens die bekend zijn in Verseon en vervolgens daar aanpassen indien nodig. Tegelijkertijd kunnen de onderzoekers in hun contact met verzoekers verifiëren of de geregistreerde contactgegevens nog actueel zijn.

Scenario 2: Contactgegevens van een verzoeker onderdeel maken van een dossier.

Onderzoek de mogelijkheid om NAW gegeven bij een dossier vast te leggen in plaats van in een aparte NAW registratie. Dit heeft als voordeel dat een dossier actuele NAW gegevens heeft omdat bij elk dossier opnieuw de NAW gegevens moeten worden vastgelegd. De keerzijde is dat moeilijker wordt om veel klagers te duiden of terug te zoeken in eerdere klachten van een verzoeker en dat het voor verzoekers minder klantvriendelijk is (bij meerdere klachten steeds opnieuw de volledige NAW gegevens opvragen).

3.1.5 P.6 Het online anoniem indienen van een klacht verdwijnt.

Prioriteit	
Eigenaar	

Indien een verzoeker een klacht indient is het noodzakelijk dat er contact kan worden opgenomen met de verzoeker. Anoniem indienen van een klacht is daarom niet van toepassing.

Advies:

Geen wijziging nodig op het klachtenformulier. Anoniem indienen van een klacht duidt op een signaal. Signalen kunnen via andere kanalen worden ingediend.

3.1.6 P.8 Gebruik persoonsgegevens voor structurele aanpak (SA) heeft een ander doel

Prioriteit	
Eigenaar	

Voor SA worden persoonsgegevens uit klachtendossiers gebruikt voor analyse en (geanonimiseerde) voorbeelden. Dit is een ander gebruik dan waarvoor de gegevens zijn verzameld. Hierover is de burger niet geïnformeerd en hiervoor is geen toestemming gevraagd.

Advies:

De structurele aanpak is een wettelijke taak van de No. Hiervoor is geen toestemming benodigd. Welk moeten verzoekers worden geïnformeerd over dit gebruik. Informatie hierover kan worden opgenomen in het privacy statement op de website.

3.1.7 P.11 informatiedeling met organisaties

Prioriteit	
Eigenaar	

Bij bemiddelen in of behandelen van klachten wordt veelal contact opgenomen met organisaties. Hierbij wordt informatie gedeeld. Het risico is dat teveel persoonsgegevens worden gedeeld met die organisaties. Het is niet altijd duidelijk wat er met die gegevens gebeurt.

Advies:

Compacte gebruikersovereenkomst. Vraag is of dit haalbaar is.

3.1.8 P.12 zichtbaarheid VIP lijst

Prioriteit	Midden
Eigenaar	

De 'VIP'-lijst bevat NAW-gegevens en contactafspraken (incl. Beperkingen) van o.a. veelklagers. Het lekken van deze lijst zou stigmatiserend werken. De lijst is op dit moment voor iedereen binnen de organisatie zichtbaar via NoHow.

Advies:

Er dient een procedure rondom gebruik, toegang en bewaartermijn van VIP gegevens worden opgesteld.

3.1.9 P.13 Via NoHow zijn klachtendossiers te zoeken en in te zien

Prioriteit	
Eigenaar	

Via NoHow is het mogelijk om bepaalde gegevens van dossiers in te zien. Voor de inhoud van de dossiers moet Verseon opgestart worden waar autorisatie wordt afgedwongen.

Er zijn twee plekken op NoHow waar dossier informatie wordt getoond:

1. Onder de profielgegevens van een medewerker. Hier worden de dossiers in behandeling getoond (omschrijving, dossiernummer, naam verzoeker/intermediair).
2. Onder de activiteiten → thema → dag. Hier worden ontvangen klachten getoond. (omschrijving en dossiernummer).

Advies:

Via NoHow wordt de omschrijving van een klacht getoond, het dossiernummer en de naam van de verzoeker. Hoewel in de meeste gevallen de beschrijving geen persoonsgegevens bevat is het handig om de onderzoekers er aan te herinneren om in het klachtomschrijving veld geen persoonsgegevens op te nemen wat kan leiden tot identificatie van betrokkene.

De klacht is alleen in te zien door te klikken op de omschrijving waarna Verseon wordt geopend en de gebruiker wordt geautoriseerd. Als de medewerker niet geautoriseerd is om de klacht in te zien, zal deze niet zichtbaar worden in Verseon.

De vraag rijst wel wat het doel is van het tonen van dossierinformatie op NoHow. Indien dit geen wezenlijk doel dient is het advies om dit van NoHow te verwijderen.

3.1.10 P.14 Interne uitwisseling dossierinformatie kan leiden tot datalekken

Prioriteit	
Eigenaar	

Informatie over dossiers en klagers wordt intern gedeeld via e-mail. Kans op verkeerd adresseren binnen No (datalek) en te lang bewaren door ontvanger (opslag in e-mail).

Advies:

Implementeer een richtlijn waarin staat dat persoonsgegevens uitsluitend via Verseon mogen worden gedeeld. Via e-mail kan een Verseon link naar een zaak of stuk rondgestuurd worden. Deze kan vervolgens alleen ingezien worden als de ontvanger intern zit (of binnen het domein van de ombudsman) en de juiste Verseon autorisatie heeft. Dit voorkomt ongeautoriseerd inzien van dossiers.

3.2 Medewerkers

3.2.1 M.4 Informatie omtrent re-integratie wordt te lang bewaard

Prioriteit	Midden
Eigenaar	Bestuursbureau, MW, MVC

De informatie die door HR wordt opgeslagen in het kader van re-integratie van medewerkers wordt te lang bewaard en niet opgeschoond. Tevens wordt het niet op de juiste plek bewaard.

Advies:

Breng deze gegevens onder in P-Direkt. Vernietig de papieren dossiers en verwijder de bestanden op de G-schijf. Dit is al in actie.

3.2.2 M.8 Medewerkers zijn niet goed op de hoogte van rechten en opslag van eigen persoonsgegevens

Prioriteit	
Eigenaar	

Medewerkers zijn niet geïnformeerd over het gebruik van hun persoonsgegevens, waar deze opgeslagen, etc. Ook zijn zij niet geïnformeerd welke rechten zij hebben en hoe ze deze kunnen uitoefenen binnen de No.

Advies:

Stel een informatieblad op voor medewerkers, waarin wordt toegelicht welke persoonsgegevens de No vastlegt, waarom, met welke grondslag, welke clouddiensten worden gebruikt, in welk geografisch gebied hun gegevens worden opgeslagen en hoe zij hun rechten (bijv correctie, inzage) kunnen uitoefenen.

4 Uitgevoerde adviezen

4.1.1 P.3. Er worden meer persoonsgegevens verzameld en opgeslagen dan strikt noodzakelijk

Prioriteit	Midden
Eigenaar	BB, Mirjam Winkel (MW)

Het gaat hierbij om gegevens die door de klager worden aangeleverd per e-mail of per post die vervolgens worden gescand. Risico op onrechtmatig verwerken en grotere impact bij evt. datalekken.

Advies:

Op de website wordt in het privacy statement benadrukt om niet meer informatie toe te sturen dan strikt noodzakelijk.

Ook aan de telefoon wordt benadrukt om alleen relevante informatie toe te sturen.

4.1.2 P.9 Gebruik privé-toestel verhoogd kans op datalekken

Prioriteit	Midden
Eigenaar	ICT, Ronald Hof

Bij mobiel werken is het mogelijk een privé-toestel (smartphone of tablet) te gebruiken voor e-mail van de No. Kans op datalekken bij diefstal en verlies of malware.

Advies:

Als onderdeel van project Locatieonafhankelijk werken krijgen de medewerkers een laptop en een (zakelijke) mobiele telefoon. Beide apparaten zijn volledig onder beheer van ICT en kunnen bij diefstal onbruikbaar worden gemaakt.

De werklaptop wordt begin 2019 in bedrijf genomen. Ingebruikname van de zakelijke mobiele telefoon volgt kort daarop.

4.1.3 P.15 Dossierinformatie wordt extern gedeeld via e-mail

Prioriteit	
Eigenaar	

De meeste datalekken die tot nu toe zijn geregistreerd zijn het gevolg van verkeerd adresseren van een e-mail bericht.

Advies:

Gebruik een tool, zoals 7zip om informatie versleuteld via e-mail te versturen. Hierbij moet het uitgangspunt zijn dat versleuteling wordt toegepast wanneer een emailbericht persoonsgegevens bevatten die een risico voor betrokkenen vormen.

Als alternatief voor versleuteld gegevensuitwisseling is het ook het onderzoeken waard om naar een 'mijn Ombudsman' portaal over te stappen waarin geautoriseerd toegang tot dossiers wordt gegeven. Een dergelijk portaal zou andere problemen (zoals wisselende contactpersonen bij organisaties) ook oplossen.

4.1.4 M.5 Vrijgeven privé adressen

Prioriteit	Laag
Eigenaar	Alle afdelingshoofden

Medewerkers vragen aan HR soms privé adressen op voor het sturen van een kaartje bij gebeurtenissen (zoals geboorte van kinderen of overlijden). Hiervoor hebben de medewerkers geen toestemming gegeven en is daarom een onrechtmatige verwerking.

Advies:

Informeer medewerkers dat het delen van privé adressen door leidinggevenden en HR niet meer is toegestaan. Het registreren van toestemming kost te veel overhead. Adviseer medewerkers om onderling gegevens uit te wisselen indien zij dat op prijs stellen.

de Nationale ombudsman

Aanbiedingsformulier	
Onderwerp	Plan van aanpak implementatie AVG
Van	
Aan	Corporate overleg
Datum behandeling	1 maart 2018
Doel van bespreking	Ter besluitvorming
Beslispunten / discussiepunten	Instemmen met het plan van aanpak
Voorgeschiedenis / context	--
Samenvatting / toelichting	In onderstaande notitie zijn de stappen beschreven die nodig zijn om de AVG te implementeren.
Financiële gevolgen	Nee
Eerder behandeld in	N.v.t.
Afgestemd met	Bestuursbureau
Spelen er privacyaspecten?	Nee
Spelen er integriteitsaspecten?	Nee
Spelen er aspecten t.a.v. (informatie)beveiliging?	Nee
Mogelijke risico's/bezwaren	Mogelijk risico is dat we niet alle stappen voor 25 mei 2018 afgerond hebben en we op onderdelen niet voldoen aan de AVG. Mogelijke maatregelen die de AP kan opleggen zijn onder meer een waarschuwing, berisping of een administratieve boete.
Communicatie	Bericht op NoHow over plan van aanpak en belangrijkste punten daaruit.
OR	Ter informatie Het verwerkingenregister en het privacy beleid (zie hieronder onder stap 3) worden nadat deze zijn vastgesteld ter instemming aan de OR voorgelegd.
Bij behandeling aanwezigheid gewenst van	--
Bijlagen	0

Aanleiding

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?

De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

Implementatie in 10 stappen

De Autoriteit Persoonsgegevens (AP) heeft een 10 stappen plan ontwikkeld voor de implementatie. Deze tien stappen, met wat deze op hoofdlijnen betekenen voor de Nationale ombudsman en Kinderombudsman, staan hieronder.

Stap 1: Bewustwording

We moeten ervoor zorgen dat de relevante mensen in de organisatie op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op de huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.

- ⇒ Het plan is om op zo kort mogelijke termijn (samen met een op dit terrein deskundig bureau) voor alle medewerkers een training te organiseren over de AVG zodanig dat zij op de hoogte zijn van de nieuwe privacyregels en de impact daarvan op hun werk. Idealiter zijn op dat moment de impact van de privacyrechten voor BNo (zie stap 2) en de inventarisatie van de gegevensverwerkingen binnen BNo (zie stap 3) afgerond, zodat deze kunnen worden meegenomen tijdens de training.
- ⇒ Daarnaast is het plan om een training over de AVG structureel te organiseren voor nieuwe medewerkers als onderdeel van het inwerkprogramma.

Deze trainingen zijn niet vrijblijvend, alle medewerkers zijn verplicht deze trainingen te volgen.

Plan is om één bureau/opleidingsinstituut te contracteren dat zowel de trainingen kan verzorgen als ons in voorkomende gevallen kan voorzien van deskundig advies.

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie wij persoonsgegevens verwerken meer en verbeterde privacyrechten. Wij moeten ervoor zorgen dat zij hun privacyrechten goed kunnen uitoefenen. Het gaat om:

- het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen.
- Het recht op vergetelheid. Het recht om 'vergeten' te worden.
- Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die BNo van hen verwerkt in te zien.
- Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die BNo verwerkt te wijzigen.
- Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.
- Het recht om bezwaar te maken tegen de gegevensverwerking.

Ten slotte hebben mensen recht op duidelijke informatie over wat BNo met hun persoonsgegevens doet.

Bij het recht op dataportabiliteit moeten wij ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen. Wat het precies inhoudt, staat in de Richtlijnen inzake het recht op gegevensoverdraagbaarheid. Om onder het recht op gegevensoverdraagbaarheid te vallen, moet het gaan om persoonsgegevens die BNo verwerkt:

- met toestemming van de betrokkene
- om een overeenkomst uit te voeren waarvan de betrokkene een partij is

Voor het recht op dataportabiliteit en voor de andere privacyrechten moeten we uitzoeken wat deze precies betekenen voor BNo.

- ⇒ Zodra we dat weten, wordt de informatie over privacyrechten op de website, intranet (NoHow), kennisbank (voor het primaire proces) en Topdesk (voor de ondersteunende processen) geactualiseerd. Voor de informatie op de website geldt dat deze voor 25 mei 2018 moet worden geactualiseerd.
- ⇒ Zo nodig wordt de informatie op de website over wat wij met persoonsgegevens doen, geactualiseerd.

- ⇒ Verder worden de werkprocessen AVG proof gemaakt. Dat gebeurt op het moment dat een werkproces wordt geactualiseerd. Voor de werkprocessen van het primaire proces en de HR-werkprocessen is dat in 2018 voorzien.

Stap 3: Overzicht verwerkingen

We moeten onze gegevensverwerkingen in kaart brengen. Dit houdt in het maken van een overzicht welke persoonsgegevens we verwerken, met welk doel, waar deze gegevens vandaan komen en met wie we ze delen.

Onder de AVG hebben we een verantwoordingsplicht. Dit houdt in dat we moeten kunnen aantonen dat we in overeenstemming met de AVG handelen. Het bijhouden van een register van verwerkingsactiviteiten (verwerkingsregister) is onderdeel van de verantwoordingsplicht.

- ⇒ Met het maken van een register is een start gemaakt. Dit moet op zo kort mogelijke termijn worden afgerond.
- ⇒ Actueel houden van het register. Dit is de verantwoordelijkheid van de degene die verantwoordelijk is voor het betrokken werkproces. Deze persoon moet de functionaris gegevensbescherming informeren.
- ⇒ Verder komt er in het verlengde van het register beleid voor de omgang met persoonsgegevens. Hiermee is een start gemaakt en dit moet op zo kort mogelijke termijn worden afgerond.

Stap 4: Data protection impact assessment

Onder de AVG kunnen we verplicht zijn een zogeheten *data protection impact assessment* (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

Er moet een DPIA worden uitgevoerd als de beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. We kunnen nu alvast inschatten of we straks DPIA's moeten uitvoeren en hoe we dit gaan aanpakken.

Komt uit een DPIA naar voren dat de beoogde verwerking een hoog risico oplevert en lukt het niet om maatregelen te vinden om dit risico te beperken, dan moeten we met de AP overleggen voordat we met de verwerking starten. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangen we een schriftelijk advies van de AP.

- ⇒ Er wordt momenteel een DPIA uitgevoerd op het DMS Verseon. Zodra eventuele risico's bekend zijn, kunnen daarop maatregelen worden ingezet. Wanneer uitvoering van deze maatregelen niet direct mogelijk is, wordt hiervoor een planning gemaakt. De implementatie van de maatregelen dan wel de planning daarvan moet voor 25 mei 2018 zijn afgerond.

Stap 5: Privacy by design & privacy by default

Onder de AVG zijn privacy by design en privacy by default verplichte uitgangspunten.

- Privacy by design houdt in dat we er al bij het ontwerpen van producten en diensten voor moeten zorgen dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat we niet meer gegevens verzamelen dan noodzakelijk is voor het doel van de verwerking. En dat we de gegevens niet langer bewaren dan nodig.
- Privacy by default houdt in dat we technische en organisatorische maatregelen moeten nemen om ervoor te zorgen dat we, als standaard, alléén persoonsgegevens verwerken die noodzakelijk zijn voor het specifieke doel dat we willen bereiken.

We moeten ervoor zorgen dat de organisatie vertrouwd raakt met deze uitgangspunten en nagaan hoe we deze beginselen binnen de organisatie kunnen invoeren.

- ⇒ Jaarlijks uitvoeren audits op privacy (circa 3 per jaar).

Stap 6: Functionaris voor de gegevensbescherming

We zijn verplicht om een functionaris voor de gegevensbescherming (FG) aan te stellen.

- ⇒ We hebben een beoogd FG, deze is echter nog niet benoemd en de benoeming moet nog ter instemming langs de OR.

- ⇒ FG aanmelden bij AP

Dit moet voor 25 mei 2018 zijn afgerond.

Stap 7: Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan onze eigen registratie van de datalekken die zich in onze organisatie hebben voorgedaan. We moeten alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of we aan de meldplicht hebben voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

De Europese privacytoezichthouders hebben in oktober 2017 guidelines gepubliceerd over de meldplicht datalekken onder de AVG. Deze guidelines zijn nog niet definitief, maar staan open voor publieke consultatie.

- ⇒ Het proces datalekken is volledig uitgewerkt. Gecheckt wordt nog of het proces in overeenstemming is met de AVG.

Stap 8: Bewerkerovereenkomsten

Wanneer we gegevensverwerking hebben uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd), dan moeten we beoordelen of de overeengekomen maatregelen in bestaande contracten met onze bewerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, dan moeten we tijdig de noodzakelijke wijzigingen aanbrengen.

- ⇒ Inkoopbeleid aanpassen.
- ⇒ Huidige overeenkomsten nalopen op overeenstemming met AVG.

Stap 9: Leidende toezichthouder

Deze stap heeft betrekking op organisaties met vestigingen in meerdere EU-lidstaten of waarvan de gegevensverwerkingen in meerdere lidstaten impact hebben? Dit geldt niet voor de No.

Stap 10: Toestemming

Voor sommige gegevensverwerkingen is toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming.

Nagaan in welke gevallen wij toestemming vragen, op welke manier we dat doen en hoe we de toestemming registreren. Zo nodig deze werkwijze aanpassen.

Nieuw is dat we moeten kunnen aantonen dat we geldige toestemming van mensen hebben gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

- ⇒ Inventariseren of BNo gegevensverwerkingen kent waarvoor toestemming nodig is van betrokkene. Voor alle gegevensverwerkingen wordt dit in kaart gebracht in het overzicht verwerkingen (zie stap 3).

Planning implementatie AVG

Stap	Activiteit	Wie	febr	mrt	apr	mei	jun	jul	aug	sept	okt	nov	dec
1. Bewustwording	Inkopen trainingen/deskundigheid												
	Training incidenteel												
	Training structureel (voor nieuwe medewerkers)												
2. Rechten van betrokkenen	In kaart brengen gevolgen privacyrechten voor BNo	 en 											
	Informatie op website actualiseren												
	Informatie op intranet (NoHow) actualiseren												
	Informatie op kennisbank actualiseren												
	Informatie in Topdesk actualiseren	Betrokken verantwoordelijke											
	Werkprocessen AVG proof maken	Betrokken verantwoordelijke											
3. Overzicht verwerkingen	Verwerkingsregister maken												
	Actueel houden register (doorlopend)	Betrokken verantwoordelijke											
	Beleid voor de omgang met persoonsgegevens	 en 											

Stap	Activiteit	Wie	febr	mrt	apr	mei	jun	jul	aug	sept	okt	nov	dec
4. Data protection impact assessment (DPIA)	DPIA Verseon												
	Plannen eventuele maatregelen												
5. Privacy by design & privacy by default	Audits op privacy (3 per jaar)	Bestuursbureau											
6. Functionaris voor de gegevensbescherming	Benoeming FG												
	Instemming OR												
	Aanmelden FG bij AP												
7. Meldplicht datalekken	Checken of proces AVG proof is												
8. Bewerkersovereenkomsten	Inkoopbeleid aanpassen												
	Checken of bestaande overeenkomst AVG proof zijn												
10. Toestemming	Zie onder 3.												

Stap 9 is niet van toepassing op BNo.

Besluit van de directeur van de Nationale ombudsman van ... maart 2018, nummer 1247284, tot aanstelling van een functionaris voor de gegevensbescherming

De directeur van de Nationale ombudsman

Overwegende dat per 25 mei 2018 de Algemene verordening gegevensbescherming (AVG) in werking treedt (EU verordening nr. 2016/679 van 27 april 2016).

Overwegende dat de Nationale ombudsman op grond van die AVG verplicht is een functionaris voor de gegevensbescherming aan te stellen.

Overwegende dat de directeur bevoegd is om die functionaris aan te stellen.

Besluit:

Artikel 1

Over te gaan tot het aanstellen van een functionaris voor de gegevensbescherming per 25 mei 2018.

Artikel 2

Tot functionaris voor de gegevensbescherming aan te stellen  , medewerker van Caesar Groep te Utrecht en op inhuurbasis werkzaam bij de organisatie van de Nationale ombudsman.

Artikel 3.

De functionaris voor de gegevensbescherming is onafhankelijk en bepaalt zelf zijn werkwijze.

De directeur van het Bureau Nationale ombudsman,

P. Tunnisen

de Nationale ombudsman

Aanbiedingsformulier	
Onderwerp	Aanstelling van een functionaris voor de gegevensbescherming
Van	■■■■■ J
Aan	Corporate overleg
Datum behandeling	22 maart 2018
Doel van bespreking	Ter bespreking
Beslispunten / discussiepunten	Voorstel t.a.v. vormen expertise groep op het terrein van de AVG.
Voorgeschiedenis / context	Met de inwerkingtreding van de AVG per 25 mei 2018 is de No verplicht een functionaris voor de gegevensbescherming (FG) aan te stellen.
Samenvatting / toelichting	Als zodanig wordt aangesteld ■■■■■ J. Dat hij niet in dienst is van de No is geen beletsel voor zijn aanstelling. ■■■■■ J valt hiërarchisch onder ICT. Omdat het onderwerp privacy bij het Bestuursbureau ligt, wordt hij op dit onderwerp functioneel aangestuurd door het Bestuursbureau. Voorstel is dat ■■■■■ J dit gaat doen samen met andere medewerkers binnen de organisatie (1 per onderdeel en AVG geschoold). Deze medewerkers fungeren als expertise groep en als liaison tussen de FG en de organisatieonderdelen. Voordelen hiervan zijn dat de kennis niet slechts bij één persoon aanwezig is (minder kwetsbaar), de FG niet alle contacten met de organisatie zelf hoeft te onderhouden en de informatiestroom vanuit de onderdelen aan de FG over de AVG (denk bijv. aan informatie over verwerkingen van persoonsgegevens) geborgd is. Privacy is immers van ons allemaal.
Financiële gevolgen	Nee
Eerder behandeld in	N.v.t.
Afgestemd met	N.v.t.
Spelen er privacyaspecten?	Nee
Spelen er integriteitsaspecten?	Nee
Spelen er aspecten t.a.v. (informatie)beveiliging?	Nee
Mogelijke risico's/bezwaren	Geen
Communicatie	Intern: NoHow Extern: Aanmelden bij AP
OR	Instemming
Bij behandeling aanwezigheid gewenst van	--
Bijlagen	Aanstellingsbesluit

Per 25 mei 2018 is de No o.g.v. de AVG verplicht een functionaris voor de gegevensbescherming te hebben. Deze verplichting geldt voor iedere overheidsinstantie of –orgaan. De functionaris voor gegevensbescherming (FG) houdt intern toezicht op en adviseert over de toepassing en naleving van de Verordening door BNo.

Taken FG

1. De FG heeft allereerst een informerende en adviserende rol binnen BNo. De FG adviseert de directeur, leidinggevend en medewerkers van BNo over de wijze waarop BNo aan de verplichtingen op grond van de Verordening, de Uitvoeringswet en andere relevante nationale of Europese regelgeving met betrekking tot de bescherming van persoonsgegevens kan voldoen.
2. De FG ziet toe op de naleving van de Verordening en andere nationale of Europese regelgeving met betrekking tot de bescherming van persoonsgegevens en op het door BNo vastgestelde beleid voor de bescherming van persoonsgegevens. Dit toezicht ziet onder meer op de vraag of voldaan wordt aan verplichtingen omtrent:
 - het toewijzen van verantwoordelijkheden
 - het bewustmaken en opleiden van het bij de verwerking betrokken personeel
 - het uitvoeren van audits

De FG verzamelt ten behoeve van het toezicht informatie om verwerkingsactiviteiten te identificeren, te analyseren en te beoordelen. Op grond daarvan voorziet de FG de organisatie van informatie, advies en aanbevelingen rondom de naleving van de Verordening bij de verwerkingsactiviteiten door BNo.

3. Op verzoek adviseert de FG over de Data Protection Impact Assessment (DPIA). Het gaat dan om:
 - de noodzakelijkheid van het uitvoeren van een DPIA
 - de methodologie
 - of u de beoordeling zelf kunt uitvoeren of dit beter door een externe partij kan worden gedaan
 - of een DPIA goed is uitgevoerd
 - of op basis van de uitkomsten nakoming van de Verordening is gewaarborgd wanneer de voorgenomen verwerking wordt gestart en of de Autoriteit Persoonsgegevens moet worden geraadpleegd
 - welke maatregelen en waarborgen bij die verwerking dienen te worden genomen

J. De FG is de schakel tussen BNo en de Autoriteit Persoonsgegevens (AP). Hoewel de FG gehouden is tot geheimhouding dan wel vertrouwelijkheid met betrekking tot de uitvoering van zijn taken, belet dat deze niet om met de AP overleg te plegen en advies te vragen omtrent de uitleg van bepaalde onderdelen van de Verordening.

Verder treedt de FG op als contactpunt voor de AP in het geval door BNo een zogenaamde voorafgaande raadpleging is aangevraagd¹.

Ook treedt de FG als contactpunt op wanneer de AP toegang vordert tot documenten of informatie ten behoeve van haar toezichthoudende taken en in de uitoefening van haar bevoegdheden.

5. De FG brengt rechtstreeks verslag uit aan de directeur van BNo. Daarnaast kan de FG ook jaarlijks een verslag uitbrengen van de door hem uitgevoerde activiteiten en deze ter beschikking stellen aan de directeur.

¹ Wanneer uit de DPIA blijkt dat een voorgenomen verwerking een hoog risico inhoudt voor de mensen van wie gegevens worden verwerkt en dit risico niet wordt weggenomen door het treffen van maatregelen, dan moet de voorgenomen verwerking worden voorgelegd aan de AP.

Meer specifiek zijn taken van de FG:

- Het maken van inventarisaties van gegevensverwerkingen.
- Bijhouden van meldingen van gegevensverwerkingen.
- Afhandelen van vragen en klachten van mensen binnen en buiten de organisatie.
- Ontwikkelen van interne regelingen.
- Adviseren over technologie en beveiliging (*privacy by design*).
- Het leveren van input bij het opstellen of aanpassen van een gedragscode.

Functie eisen

De functie van FG moet worden vervuld door een deskundige persoon. Het benodigde niveau van kennis en expertise moet in verhouding staan tot de gevoeligheid, complexiteit en hoeveelheid persoonsgegevens die een organisatie verwerkt. De FG dient deskundig te zijn op het gebied van wetgeving en de praktijk rondom de bescherming van persoonsgegevens, waaronder een diepgaand begrip van de Verordening en de Uitvoeringswet. Verder dient hij voldoende persoonlijke kwaliteiten te bezitten om zijn taken op grond van de Verordening goed te kunnen vervullen. Dergelijke kwaliteiten zien onder meer op integriteit en professionele ethiek. Tot slot moet de FG voldoende kennis hebben van de organisatie.

De FG hoeft niet alle deskundigheden zelf te bezitten. Het is voldoende als deze deskundigheden (bijvoorbeeld door het extern inwinnen van advies) beschikbaar zijn.

Het zijn van FG binnen BNO is geen voltijds positie. De andere taken en plichten van de FG binnen BNO mogen niet conflicteren met diens taken als FG. Zo mag de FG niet ook een functie vervullen waarbij deze het doel en de middelen voor gegevensverwerkingen vaststelt.

De FG is gehouden tot geheimhouding voor wat betreft de uitvoering van zijn taken. In het bijzonder is de FG gehouden tot geheimhouding van hetgeen hem op grond van klachten of verzoeken van een betrokkene ter ore komt, tenzij de betrokkene instemt met bekendmaking. De FG moet dus betrouwbaar zijn.

De functionaris voor de gegevensbescherming is niet eindverantwoordelijk voor de naleving van de Verordening. De verwerkingsverantwoordelijke blijft eindverantwoordelijk voor de goede naleving van de Verordening. De FG wordt geraadpleegd en houdt toezicht, maar is niet de degene die uiteindelijk de beslissing neemt over het al dan niet verwerken van persoonsgegevens of het nemen van maatregelen.

Waarborgen

Voor het goed kunnen uitoefenen van de functie van FG is in de volgende waarborgen voorzien.

- De FG dient onafhankelijk zijn rol te kunnen vervullen. Dit betekent dat aan de FG geen instructies mogen worden gegeven. De FG dient zich een onafhankelijke visie te kunnen vormen over de uitleg van de Verordening.
- De FG heeft een vorm van ontslagbescherming: de FG kan niet ontslagen of gestraft worden voor de uitvoering van zijn taken.
- De FG wordt tijdig en behoorlijk betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Om te waarborgen dat de FG inderdaad op tijd en in voldoende mate wordt betrokken, wordt de FG:
 - Uitgenodigd om aan vergaderingen van de leiding van BNO deel te nemen zodra daar aangelegenheden besproken worden die verband houden met de bescherming van persoonsgegevens.
 - Uitgenodigd wanneer in ander verband beslissingen met gevolgen voor de gegevensbescherming worden genomen.
 - Onmiddellijk geraadpleegd indien zich een datalek of ander incident voordoet.

- Wordt tegen het advies van de FG in een besluit genomen dat naar zijn oordeel in strijd is met de Verordening, dan kan de FG zijn advies voorleggen aan de directeur van BNo. Bij verschil van inzicht wordt vastgelegd waarom het advies van de FG niet is gevolgd.
- De FG heeft toegang tot persoonsgegevens en verwerkingsactiviteiten zodat de FG zelf kan onderzoeken welke verwerkingsactiviteiten plaatsvinden en of deze voldoen aan de vereisten van de Verordening.
- Verder worden de middelen ter beschikking gesteld die de FG nodig heeft om zijn taken te vervullen. Deze middelen zijn bijvoorbeeld: voldoende tijd om zijn taken uit te voeren, financiële middelen en (bij)scholing.
- Mensen van wie door BNo gegevens worden verwerkt (betrokkenen) moeten contact kunnen opnemen met de FG. Betrokkenen moeten zich kunnen wenden tot de FG voor alle aangelegenheden die verband houden met de Verordening, in het bijzonder daar waar het de uitoefening van hun rechten op grond van de Verordening betreft.

FG aanmelden bij AP

De FG moet worden aangemeld bij de AP. Pas dan kan de FG als zodanig aan de slag.

Van: [REDACTED] 
Verstuurd: Wed, 7 Mar 2018 10:58:04 +0100
Aan: .Alle medewerkers
Onderwerp: Privacy en AVG

Beste collega's,

Vanaf 25 mei is de Algemene Verordening Gegevensverwerking (AVG) van toepassing. Vanaf die datum geldt dezelfde privacy regeling in de gehele Europese Unie. De Wet Bescherming Persoonsgegevens geldt vanaf dan niet langer.

In afwachting van de AVG wordt er door het Bestuursbureau het nodige voorbereid en op NoHow gepubliceerd. Ook staat er een training voor alle medewerkers op het programma om een ieder vertrouwd te maken met de nieuwe regelgeving en de gevolgen daarvan voor ons werk.

Vragen over Privacy

Heb je al concrete vragen over de toepassing van privacy regelgeving in je dagelijkse werk, stel die vragen dan gerust aan het Bestuursbureau. Op grond van de vragen die wij van jullie ontvangen, wordt een overzicht met veel gestelde vragen met antwoorden op NoHow gepubliceerd.

Met vriendelijke groet,

[REDACTED] 

Wat gaat er veranderen t.o.v. nu?

Door de algemene verordening gegevensbescherming (AVG) krijgen mensen meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun gegevens. Hun privacyrechten worden versterkt en uitgebreid. Naast versterking van de bestaande rechten (recht om in te zien, recht om te wijzigen en recht op informatie) krijgen mensen door de AVG een aantal aanvullende rechten: recht op vergetelheid en recht op dataportabiliteit.

Organisaties krijgen meer verplichtingen bij het verwerken van persoonsgegevens. Dit geldt ook voor de ombudsman.

- Zo moeten wij met documenten kunnen aantonen dat wij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG te voldoen (verantwoordingsplicht).
- Verder zijn wij verplicht een functionaris voor de gegevensbescherming aan te stellen.
- Tot slot zijn we in sommige gevallen verplicht een zogenaamde 'Data protection impact assessment' uit te (laten) voeren.

Hier staat tegenover dat we vanaf 25 mei 2018 verwerkingen van persoonsgegevens niet meer hoeven te melden bij de Autoriteit Persoonsgegevens. Alle verwerkingen moeten per die datum wel zijn vastgelegd in het verwerkingsregister.

Wat onveranderd blijft, is dat er een beperkt aantal gronden is op basis waarvan persoonsgegevens mogen worden verzameld. Onder de AVG zijn dit: toestemming van de gebruiker, vitale belangen, wettelijke verplichting, overeenkomst, vervulling taak in het algemeen belang of uitoefening openbaar gezag en gerechtvaardigd belang. Deze gronden zijn gelijk aan op de gronden genoemd in de Wet bescherming persoonsgegevens. In dit opzicht verandert er dus niets.

Wat moet ik straks anders gaan doen?

Het gaat niet zozeer om anders, eerder om bewuster. Wees je ervan bewust dat je met persoonsgegevens werkt. Vraag jezelf bij het opvragen van gegevens altijd af of je in een fase van de verzoekbehandeling zit waarin je gegevens mag opvragen en of je de gegevens echt nodig hebt om een verzoek te kunnen behandelen. Vraag nooit om meer gegevens dan je echt nodig hebt.

Ook voor het vastleggen van gegevens in Verseon geldt: sla nooit meer gegevens op dan moet (op grond van de Archiefwet) of mag (op grond van de AVG).

Hoe verhoudt de AVG zich tot de Archiefwet?

Op grond van de Archiefwet zijn wij verplicht bepaalde persoonsgegevens te registreren. Denk bijvoorbeeld aan de persoonsgegevens van iemand die ons een brief stuurt. We moeten voldoende gegevens registreren om de brief makkelijk te kunnen vinden en raadplegen¹. We mogen op grond van de AVG niet meer gegevens registreren dan daarvoor (of voor de verzoekbehandeling) nodig is.

Mag je documenten nog in je kast bewaren?

We werken digitaal, maar als je documenten geprint hebt, mag je die in je kast blijven bewaren. Dit geldt ook voor dossiers die je uit het archief hebt laten halen. Zorg er wel voor dat je die kasten afsluit op het moment dat je weggaat zodat onbevoegden er niet bij kunnen.

Welke gegevens mogen wij opvragen?

Op grond van de AVG moet elke verwerking van persoonsgegevens voldoen aan de volgende beginselen²:

¹ Het gaat hier om het verwerken van persoonsgegevens om te voldoen aan een wettelijke plicht.

² Meer hierover kun je lezen in de Handleiding AVG paragraaf 2.4..

- De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn.
- De verwerking moet gebonden zijn aan specifieke verzameldoelen.
- De persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is.
- De gegevens moeten juist zijn.
- De gegevens mogen niet langer worden bewaard dan nodig.
- Gegevens moeten goed beveiligd zijn en vertrouwelijk blijven.

Op grond van artikel 9.18 van de Awb zijn wij verplicht verzoeken tot het instellen van een onderzoek te behandelen. Deze bepaling is de grondslag voor het opvragen van persoonsgegevens in het kader van de verzoekbehandeling.

Als algemene richtlijn kun je aanhouden dat je in de eerste fase van de behandeling (toetsing bevoegdheid en ontvankelijkheid) alleen die informatie mag opvragen die je nodig hebt om deze toets te kunnen uitvoeren. Doorstaat een verzoek deze toets en wordt besloten tot het instellen van een onderzoek (interventie, bemiddeling of schriftelijk onderzoek) dan mag je alle informatie opvragen die nodig is om de interventie of de bemiddeling in te zetten en af te ronden of om ingeval van een onderzoek een oordeel te kunnen geven over de klacht.

Soms stellen we een zogenaamd vooronderzoek in. Een vooronderzoek heeft tot doel vast te stellen of we wel/niet een onderzoek gaan instellen. Tijdens zo'n vooronderzoek mogen we dan ook alleen gegevens opvragen die we daarvoor nodig hebben. We mogen in deze fase geen informatie opvragen om vast te kunnen stellen of de gedraging waar het om gaat behoorlijk is of niet. Die informatie mogen we alleen opvragen als we een onderzoek instellen.

Is het doorsturen van kennelijk ongegrond brieven toegestaan?

Voor het doorsturen van kennelijk ongegrond brieven aan overheidsinstanties bestaat geen wettelijke grondslag. We mogen dit zonder toestemming van betrokkene niet doen. We mogen dit wel doen wanneer we de brief anonimiseren zodanig dat deze niet meer tot de betrokken persoon herleidbaar is. Een optie is ook om de boodschap die we met het doorsturen van de brief willen overbrengen op een andere manier over te brengen.

Voor welke soortgelijke gevallen geldt dit nog meer?

Dit geldt voor alle brieven waarin wij aan een verzoeker meedelen dat we geen onderzoek gaan instellen, op welke grond dan ook. Zie ook artikel 9:25 Awb.

Wanneer mogen wij Informatie inwinnen bij overheidsinstanties?

Wanneer iemand een verzoekschrift bij ons indient, moet betrokkene er op kunnen vertrouwen dat wij zorgvuldig met zijn/haar persoonsgegevens omgaan. Dit betekent onder meer dat betrokkene er op moet kunnen vertrouwen dat we derden niet informeren over zijn/haar klacht. Dat geldt ook voor de betrokken overheidsinstantie(s).

Heb je meer informatie nodig om iemands verzoek te kunnen behandelen, dan vraag je die informatie in eerste instantie altijd op bij betrokkene zelf. Pas als deze die informatie niet (meer) heeft mag je de betrokken overheidsinstantie informeren over het verzoek en informatie voor de behandeling daarvan opvragen. Je kunt de verzoeker hiervan op de hoogte brengen. Let op: je mag niet meer informatie opvragen dan je nodig hebt om het verzoek te kunnen behandelen. Het is dus bijv. niet toegestaan zonder meer een heel intern klachtdossier op te vragen zonder dat je weet welke informatie daarin is opgenomen.

Is eenmaal besloten een onderzoek in te stellen dan zijn wij op grond van artikel 9:30 Awb verplicht het betrokken bestuursorgaan en degene op wiens gedraging het verzoek betrekking heeft in de

gelegenheid te stellen hun standpunt toe te lichten. Voor een goede uitvoering van het beginsel van hoor en wederhoor is nodig dat zij in dat kader kennis kunnen nemen van het verzoek. Voor het toesturen daarvan is dus een duidelijke wettelijke grondslag.

Verder zijn het bestuursorgaan, (gewezen) medewerkers en getuigen op grond van artikel 9:31, eerste lid, Awb verplicht de ombudsman de benodigde inlichtingen te verstrekken. Tot slot staat in het derde lid van dit artikel dat het bestuursorgaan, degene op wiens gedraging het verzoek betrekking heeft en anderen onder hen berustende stukken aan de ombudsman moeten overleggen nadat hij hierom schriftelijk heeft verzocht.

Bijzondere categorieën van persoonsgegevens

Bijzondere categorieën van persoonsgegevens mogen in beginsel niet worden verwerkt. De Nederlandse uitvoeringswet (wetsvoorstel) kent hierop in artikel 23 onder meer als uitzondering de verwerking door de Nationale ombudsman:

- voor zover de verwerking noodzakelijk is voor de uitvoering van de hem wettelijk opgedragen taken, en
- onder voorwaarde dat bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Kortom: zolang je bezig bent met de uitvoering van de aan de No wettelijk opgedragen taken, en je informatie opvraagt die je echt nodig hebt om die taken te kunnen uitvoeren, heb je geen toestemming nodig van verzoeker om zijn/haar (bijzondere) persoonsgegevens te verwerken.

Wanneer mogen wij informatie inwinnen bij andere (overheids)instanties?

In artikel 9:31, derde lid, Awb staat dat ook 'anderen' onder hen berustende stukken aan de ombudsman moeten overleggen nadat hij hierom schriftelijk heeft verzocht. Dit betekent dat wij ook bij andere (overheids)instanties informatie kunnen opvragen in het kader van een onderzoek.

Door wie zijn intern de verzoekdossiers in te zien?

Momenteel wordt onderzocht hoe de rechten op verzoekdossiers anders kunnen worden ingericht, waardoor minder mensen bij alle informatie kunnen. Momenteel kunnen de dossiers onderverdeeld worden in dienstgeheim, vertrouwelijk en geheim. Dossiers en documenten die op dienstgeheim staan, zijn voor de hele organisatie toegankelijk. Dossiers en documenten die op vertrouwelijk staan, zijn alleen binnen het onderdeel in te zien. De dossiers en documenten die op geheim staan, zijn alleen toegankelijk voor gescreende medewerkers die o.a. dossiers van de AIVD behandelen.

Hoe om te gaan met versleutelde berichten; wanneer moeten wij onze berichten versleuteld versturen?

Binnen ons werk of het nu over klachtbehandeling gaat, informatiebeveiliging of over verzending van stukken m.b.t. personeel; we hebben allemaal te maken met vertrouwelijke en gevoelige informatie. Daarom moeten we elke keer als we iets verzenden zelf de afweging maken of deze informatie extra moet worden beschermd met versleutelde verzending via de mail met 7-Zip of niet. Dit ter voorkoming van een datalek.

Als je mailt binnen de Rijksoverheid, wordt hiervoor een apart netwerk gebruikt (de Haagse Ring), daarom is het over het algemeen niet nodig om gebruik te maken van 7-Zip tenzij...

Wanneer gebruik maken van 7-Zip met gebruik van wachtwoord:

- Als je gebruik maakt van bv een systeem als We Transfer om grote hoeveelheid aan bestanden te mailen.
- Als je mailt buiten de Rijksoverheid en het betreft gevoelige en vertrouwelijke informatie.

- Als je mailt binnen de Rijksoverheid en je vermoed dat de informatie bij meerdere personen terecht komt, waarvoor de informatie niet is bedoeld.
- Als je mailt binnen de eigen organisatie en je vermoed dat de informatie door meerdere personen kan worden ingezien, waarvoor de informatie niet is bedoeld.

Zie ook: [Wat betekent de Wet datalekken voor ons? - NoHow](#)

Het allerbelangrijkste is, blijf alert en beoordeel bij het verzenden van elke mail of beveiligd verzenden noodzakelijk of wenselijk is.

Wat is 7-zip en hoe kan ik dit gebruiken

7-zip is een mogelijkheid om documenten in te pakken en veiliger te verzenden. Ook worden de bestanden verkleind, waardoor je meer bestanden per mail kunt verzenden.

Hoe werkt het:

- Open 7-zip op je bureaublad en selecteer vervolgens de bestanden en sleep deze naar 7-zip. Kijk hier voor de tips en trucs m.b.t. [Verseon en Bureaudok](#)
- Als je documenten vanaf je G of H-schijf wilt verzenden, kun je ook direct de te verzenden documenten selecteren. Vervolgens klik op je rechtermuisknop en klik je vervolgens op 7-zip.
- Kijk in de [handleiding](#) voor meer informatie over het inpakken en openen van documenten en andere bestanden.
- Speek met ontvangers van de mail een wachtwoord af voor een bepaalde periode, en doe dit niet in dezelfde mail waarin het 7-zip bestand zit.
- Zorg ervoor dat je het wachtwoord in het dossier documenteert zodat je altijd het 7-zip bestand kunt openen.

Gebruik van 7-zip in mail aan verzoekers

Wil je gebruik maken van 7-zip bij het sturen van gevoelige of vertrouwelijke informatie aan verzoekers, ga dan van te voren na of verzoeker weet hoe dit werkt.

To do lijst AVG

2.4 De contactgegevens van de FG zijn te vinden op het intranet en de website van de Nationale ombudsman.

2.6 Bezoekers van het gebouw van de No moeten worden dat er cameratoezicht is.

2.6 en 4.9 Uitzoeken of wij disclaimer willen gebruiken en waarvoor precies.

2.6 Burgers en organisaties in de ontvangstbevestiging van brieven e.d. informeren dat zij bezwaar kunnen maken tegen opname van hun gegevens in Verseon. Uitzoeken hoe dit zich verhoudt tot Archiefwet. Mogen we bijv. als iemand dit niet wil de brief van betrokkene terugsturen?

3.5 Op het intranet van de Nationale ombudsman zijn de regels omtrent archiveren te vinden.

4.4 Er is een procedure ingericht om te zorgen dat betrokkenen hun rechten kunnen uitoefenen. Dit wordt duidelijk en transparant gecommuniceerd, zowel op het intranet als op het internet.

Incompany cursus AVG 2018



INCOMPANY : TRAININGEN OP MAAT VOOR JE TEAM

UW VRAAG

Beste 

Bedankt voor je vraag om voor de verantwoordelijke medewerkers van de Nationale Ombudsman een 2-daags programma op te stellen om zo samen te leren hoe om te gaan met de nieuwe privacy wetgeving. Naast wat algemene kennis over de AVG zullen we ook samen kijken naar de specifieke werkzaamheden van de nationale Ombudsman en de invloed van de wetgeving daarop. Mogelijke aanpassing van protocollen en behandeling eigen casuïstiek van de Nationale Ombudsman.

Het definitieve programma zal worden vastgesteld in overleg met de aanvrager en de (hoofd)docent.

ALGEMENE PUNTEN

Termijn	Start voorjaar 2018
Duur van het traject	4 dagdelen
Tijdschema	Voorgestelde tijden (in overleg aan te passen): 9.00 uur welkom 9.30 uur start 16.30 uur einde Tijdens de dag zijn er koffie en theepauzes, en een lunchpauze
Locatie	Op locatie Nationale Ombudsman
Aantal deelnemers	max 16 personen

Benodigde apparatuur & techniek *(in overleg af te stemmen samen met de trainer)*

- Trainingslocatie
- Projectiescherm, Flip-over, Beamer, laptop
- Bij voorkeur wordt er gewerkt met tafels in "U-vorm", met daarvoor een tafel voor de docent & beamer.

Op verzoek kunnen wij dit voor u verzorgen, wij hebben dit niet meegenomen in de offerte.

DE OPLEIDING

Opbouw programma

Het definitieve programma van deze opleiding wordt samengesteld in overleg met de opdrachtgever en de docenten. Ook worden door uzelf aangeleverde casuïstiek behandeld door de docenten tijdens de opleiding. Op deze manier vormt de aanwezige kennis, ervaring en de lokale praktijk het uitgangspunt voor de bijdrage van de docenten.

Tijdens de opleiding worden verschillende werkvormen gehanteerd door de docenten. Zo wordt er niet alleen gedoceerd, maar gaan de deelnemers ook zelf aan de slag met de eigen casuïstiek.

Dag 1

De toepassing en reikwijdte van de AVG

- Wat is een persoonsgegeven en wat niet? Wat is een bestand?
- Wat valt onder de uitzondering van persoonlijke of huishoudelijke doeleinden?
- Wat geldt er m.b.t. journalistieke verwerkingen?
- Wanneer is de Nederlandse privacywet van toepassing en wanneer niet?
- Wat verandert er door de Algemene Verordening Gegevensbescherming?

De werking van de AVG

- Wat mag wel en wat mag niet met persoonsgegevens?
- Wat is een welbepaald verzameldoel en wat betekent niet-onverenigbaar?
- Hoe lang mogen gegevens worden bewaard?
- Wanneer moet inzage worden gegeven in klantgegevens?
- Hoe ver gaat de informatieplicht? Wat is het vergeetrecht?
- Moeten foto's en beeldopnamen worden aangemerkt als rasgegevens?
- En wat zeggen de nieuwe richtsnoeren over cameratoezicht daarover?
- De WP29 opinies over de FG en gegevensoverdraagbaarheid

Beveiliging en meldplicht datalekken, toezicht en handhaving door de AP

- Welke bevoegdheden heeft de toezichthouder?
- Wat is het handhavingsbeleid van de AP?
- Goedkeuring van gedragscodes
- Welke bestuurlijke boetes kan de toezichthouder opleggen?
- Wat verandert er als gevolg van de Algemene Verordening Gegevensbescherming?

De Nationale Ombudsman; beleid en regels

- Intern beleid betreffende privacy
- Regels en protocol

Dag 2

De Nationale Ombudsman en de nieuwe wetgeving

- Interne processen
- Risico's van de nieuwe wetgeving
- Interne vragen
- Verwerkingsregister
- Behandeling zelf ingebrachte casuïstiek

UW DOCENT

dr. [REDACTED] J, CIPP/E CIPM CIPT » partner

[REDACTED] J, van huis uit informaticus, kan zich als het gaat over privacywetgeving met de besten meten. Die kennis deed hij op als privacy adviseur en trainer, en eerder bij de Autoriteit Persoonsgegevens. [REDACTED] J is bekend met beleidsprocessen bij de overheid, politiek sensitief en altijd op zoek naar oplossingen die zowel gedegen als pragmatisch zijn. Klanten waarderen hem om zijn open, flexibele en resultaatgerichte instelling, zijn kennis van zaken en om zijn vermogen om ingewikkelde zaken eenvoudig te maken, zowel in woord als in geschrift.

KWALITEITSBORGING

Werkvormen

Tijdens de opleiding worden verschillende werkvormen gehanteerd door de docenten. Zo wordt er niet alleen gedoceerd, maar gaan de deelnemers ook zelf aan de slag met de eigen casuïstiek.

Ook worden door uzelf aangeleverde casuïstiek behandeld door de docenten tijdens de opleiding. Op deze manier vormt de aanwezige kennis, ervaring en de lokale praktijk het uitgangspunt voor de bijdrage van de docenten.

Coaching op de werkplek en intervisie/terugkomdag zijn ook beproefde methoden van borging; in overleg plannen we deze in binnen 6 maanden na de Incompany opleiding.

Het is tot 2 jaar na de opleiding mogelijk via de online leeromgeving contact met de docent te onderhouden.

Online leeromgeving

Om de opleiding meer didactische mogelijkheden te bieden, maken wij gebruik van een online leeromgeving. Hieronder treft u meer informatie aan over de toepassingen en het gebruik van deze leeromgeving.

De online leeromgeving wordt gebruikt door de deelnemers, organisatie en docenten. Het is een interactieve tool waarop deelnemers alle praktische informatie, presentaties, theorie, artikelen, eventuele huiswerkopdrachten en verwijzingen naar boeken kunnen downloaden.

Deelnemers en docenten kunnen direct met elkaar in contact komen vóór, tijdens en ná de opleiding.

Voorafgaand aan de opleiding vragen wij deelnemers via de leeromgeving een voorbereidingsopdracht en/of intake in te vullen zodat zowel deelnemers als de docent zich goed kunnen voorbereiden op de opleiding. Op deze manier kunnen de docenten bij hun bijdrage aan de opleiding (indien nodig en mogelijk) anticiperen op de verschillende achtergronden en kennisniveaus van de deelnemers aan de opleiding.

Evaluatie

Naast de intake vindt ook de evaluatie via de online leeromgeving plaats. Dit gebeurt niet alleen na afloop van de opleiding. Ook tijdens de opleiding hebben de deelnemers de mogelijkheid om een tussentijdse evaluatie in te vullen. Op die manier kunnen wij de kwaliteit van het programma bewaken en (indien nodig en mogelijk) anticiperen op (extra) kennisbehoeften van de deelnemers aan de opleiding.

Kortom:

- De online leeromgeving geldt als een actueel naslagwerk
- De onlineleeromgeving gebruikt u als netwerkinstrument en voor interactie: alle deelnemers en docenten zijn via de leeromgeving snel te bereiken voor en na de bijeenkomst
- De deelnemers kunnen alle informatie voorafgaand aan iedere lesdag downloaden of eventueel uitprinten
- De leeromgeving is toegankelijk vanaf iPad, e-reader of laptop

ONZE AANPAK

Om deze Incompany training tot een succes te maken, is een goede voorbereiding en planning vereist.

FASE ACTIE

1. Trainingsbehoefte in beeld

Allereerst vindt er een (telefonische) intake plaats. Dit is een gesprek waarin één van onze accountmanagers uw trainingsbehoeftes uitvoerig met u doorneemt.

2. Ons voorstel

Na dit intake gesprek ontvangt u van ons een passende offerte.

3. Afstemming

Persoonlijk (telefonisch) intakegesprek met de trainer en/of accountmanager op een nader te bepalen datum.

4. Voorbereiding

- Vaststellen van definitief programma & trainingsdata en tijden
- Organisatie locatie en uitnodigen van deelnemers (klant)
- Aanleveren deelnemerslijst (klant)
- Voorbereiden onlineleeromgeving & versturen van het opleidingsmateriaal

5. Uitvoering training

6. Mondelinge en schriftelijke Evaluatie

Op de laatste dag van de training vult iedere deelnemer een digitaal evaluatieformulier in. Binnen twee weken na de training neemt de accountmanager contact met u op om de bevindingen te bespreken. In dit gesprek worden de volgende vragen behandeld.

- Wat zijn de ervaringen van de deelnemers na de training?
- Wat zijn de aannames/wensen na de training?
- Zijn de doelstellingen behaald?
- Mogelijkheden verdiepingsdag?

INVESTERINGSVOORSTEL

Dit voorstel is gebaseerd op max. 16 deelnemers

Vorbereiding van de trainer en Studiecentrum voor Bedrijf en Overheid

- Intake
- Programma afstemming
- Evt. Huiswerkopdracht
- Inrichten online leeromgeving

Inclusief

- Notitieblok, pen, naambordjes
- Certificaat van deelname (digitaal)
- Aflevering van het materiaal
- Toegang tot de online leeromgeving
- Reiskosten trainers

Exclusief

- Aanbevolen maar niet noodzakelijk studiemateriaal (optioneel)

Prijs voor 4 dagdelen training



Deze offerte heeft een geldigheid van drie maanden.

OVER ONS

Het Studiecentrum voor Bedrijf en Overheid (onderdeel van Euroforum BV.) heeft zich gespecialiseerd in het ontwikkelen van kwalitatief hoogwaardige opleidingen, cursussen en workshops. Daarbij werken we samen met gerenommeerde adviesorganisaties op het gebied van onder andere sociale zekerheid en gezondheidszorg, ruimtelijke ordening, bestuur en milieu. De bijeenkomsten zijn speciaal ontwikkeld voor beleidsmakers en het (hoger) management binnen overheid, non-profit en het bedrijfsleven.

Onze trainers zijn veelal mensen uit de praktijk, die hun ervaringen omzetten naar de theorie. Zij zijn erop gericht om de deelnemers te laten vertellen over hun eigen praktijkervaringen en gedachten zodat er inzicht en commitment wordt gecreëerd. Onze opleidingsmethode wordt ondersteund door o.a. een digitale leeromgeving met daarin de theorie, praktijkopdrachten, presentaties en praktische tools.

Naast onze open opleidingen organiseren wij ook Incompany opleidingen. Deze opleidingen worden naar aanleiding van de vraag en doelstelling op maat ontwikkeld. Hiermee kunnen wij een programma nog specifiek op de organisatie en de medewerkers afstemmen. Het resultaat is gemotiveerde medewerkers, verhoogde teamspirit en verbeterd resultaat!

De voordelen op een rij

- Het betreft een speciaal voor u opgezette opleiding, verzorgd door professionals uit de praktijk.
- Geen extra reiskosten en tijdsbeslag voor de deelnemers.
- De grootte van de groep stimuleert de interactiviteit.
- De onderlinge betrokkenheid en motivatie stijgen aantoonbaar.
- Het hele team in één keer op hetzelfde kennisniveau.
- De opleiding wordt gegeven wanneer het u uitkomt.
- Aanmerkelijk prijsvoordeel in vergelijking met een individuele opleiding.

Kijk voor ons overige opleidingsaanbod op onze website, www.sbo.nl

Contactgegevens:

Voor vragen en opmerkingen over ons voorstel kunt u contact opnemen met:



Senior Manager Incompany Training

Tel.: 040 – 

Mob: 06 – 

E-mail: @sbo.nl

ALGEMENE VOORWAARDEN EUROFORUM B.V.

23 februari 2016

Euroforum B.V. is ingeschreven bij de Kamer van Koophandel te Eindhoven onder nummer 1707 5223
Deze algemene voorwaarden gelden voor de merken en de handelsnamen Euroforum, Secretary Management Institute, NIB (Nederlands Instituut voor de Bouw), Studiecentrum voor Bedrijf en Overheid en tevens voor European Business Studies.

Artikel 1: Definities

In deze algemene voorwaarden wordt verstaan onder:

1. Euroforum: De besloten vennootschap met beperkte aansprakelijkheid Euroforum B.V., gevestigd en kantoorhoudende te Eindhoven aan de Emmasingel 33.
2. Acceptatie: Opdracht- of aanmeldbevestiging van Euroforum gericht aan Deelnemer of Wederpartij.
3. Abonnement: Alle door of namens Euroforum uitgebrachte diensten in Abonnement(en)-vorm, zoals schriftelijke nieuwsbrieven, publicaties, literatuur en alle overige verstrekkingen.
4. Bijeenkomst: Alle door Euroforum georganiseerde bijeenkomsten waaronder in ieder geval dient te worden verstaan: Congressen, cursussen, seminars, conferenties, in company bijeenkomsten.
5. Cursus: Trainingen, opleidingen, opleidingen, masterclasses, of enige andere vorm van opleiding.
6. Deelnemer: De natuurlijke persoon die als deelnemer aan één van de Bijeenkomsten van Euroforum is aangemeld.
7. Wederpartij: De rechtspersoon die met Euroforum een dienstverleningsovereenkomst sluit.
8. Inschrijfgeld: De kosten voor deelname aan een door Euroforum georganiseerde Bijeenkomst.
9. Annulering: Als een Deelnemer of Wederpartij zich heeft ingeschreven voor een Bijeenkomst

Artikel 2: Toepasselijkheid

1. Op de door en/of aan Euroforum gedane aanbiedingen, offertes, opdrachtbevestigingen, aanmeldingen, gesloten overeenkomsten en alle door Euroforum te verrichten diensten zijn uitsluitend deze algemene voorwaarden van toepassing.
2. De toepasselijkheid van andere algemene voorwaarden wordt uitdrukkelijk en in alle gevallen van de hand gewezen ook indien naar deze voorwaarden wordt verwezen in een aan Euroforum gericht aanbod.
3. Indien enige bepaling van deze algemene voorwaarden nietig is of vernietigd wordt, zullen de overige bepalingen van deze algemene voorwaarden volledig van kracht blijven en zullen partijen met elkaar in overleg treden teneinde nieuwe bepalingen ter vervanging overeen te komen, waarbij zoveel mogelijk aansluiting wordt gezocht met het doel en de strekking van de nietige c.q. vernietigde bepaling.

Artikel 3: Aanbiedingen / Totstandkoming

1. Alle door Euroforum gedane aanbiedingen zijn vrijblijvend, tenzij anders is aangegeven en dienen met deze algemene voorwaarden als één geheel te worden opgevat.
2. Acceptatie geschiedt door een schriftelijke opdracht- of aanmeldbevestiging. Acceptatie kan tevens mondeling geschieden met uitzondering van hetgeen bepaald in artikel 16 van deze algemene voorwaarden.
3. Als gevolg van een Acceptatie bevestigt de Deelnemer en/of Wederpartij dat deze de daaruit voortvloeiende (betalings- of andersoortige) verplichtingen accepteert en derhalve gehouden is de verplichtingen na te komen behoudens in geval van een situatie zoals omschreven in dit artikel. Het al dan niet ontvangen hebben van een orderbevestiging laat de verplichtingen zoals aangegeven in dit artikel onverlet.
4. Indien door omstandigheden, waaronder vanwege de aard, omvang of de spoedeisendheid van de opdracht, geen orderbevestiging is verzonden, wordt de factuur daaraan gelijkgesteld.
5. Toezending van aanbiedingen en/of andere documentatie aan de Deelnemer en/of Wederpartij verplicht Euroforum niet tot aanvaarding van een inschrijving. Euroforum is gehouden een eventuele afwijzing van de aanvaarding zo spoedig mogelijk, maar in elk geval binnen 14 dagen aan de Deelnemer en/of Wederpartij ter kennis te brengen. Euroforum behoudt zich te allen tijde het recht voor om opdrachten zonder opgave van redenen te weigeren.
6. Elke overeenkomst wordt aangegaan onder de opschortende voorwaarde dat de Deelnemer en/of Wederpartij voldoende kredietwaardig blijkt voor de geldelijke nakoming van de overeenkomst. Wijzigingen in de overeenkomsten dienen schriftelijk door beide partijen te zijn overeengekomen.
7. Indien een aanbieding vergezeld gaat van begrotingen, planningen, catalogi of andere bescheiden, blijven deze te allen tijden eigendom van Euroforum en moeten deze op eerste verzoek worden teruggegeven. Zij mogen zonder uitdrukkelijke schriftelijke toestemming vooraf niet worden vermenigvuldigd, nagemaakt op welke wijze dan ook, of aan derden worden doorgegeven dan wel ter inzage worden gegeven.
8. Euroforum wordt uitdrukkelijk gemachtigd om, indien en voor zover Euroforum dit binnen de grenzen van de gegeven opdracht nodig of wenselijk acht, werkzaamheden door derden voor uw rekening te doen verrichten alsmede rechten en verplichtingen welke voortvloeien uit de overeenkomst aan derden over te dragen.

Artikel 4: Facturering en betaling

1. Tenzij schriftelijk anders overeengekomen dient betaling van het Inschrijfgeld uiterlijk voor aanvang van de Bijeenkomst in bezit te zijn van Euroforum, onder vermelding van het factuurnummer. De op het bankafschrift van Euroforum aangegeven valutadag is bepalend en wordt dus als dag van betaling aangemerkt.
2. In geval sprake van sponsoring conform artikel 16 van deze algemene voorwaarden wordt de termijn zoals genoemd in artikel 4 onder lid 1 vastgesteld op 40 dagen voor aanvang. In geval de factuurdatum binnen deze 40 dagen valt, wordt de termijn gesteld op 2 dagen voor aanvang.
3. Is tijdige betaling uitgebleven, dan kan de Deelnemer en/of Wederpartij de toegang tot de Bijeenkomst worden geweigerd, tenzij het verschuldigde bedrag alsnog contant wordt voldaan of wordt gestaafd middels het overleggen van een bewijs van betaling.
4. Alle door de Deelnemer en/of Wederpartij verrichte betalingen strekken primair tot voldoening van eventuele rente en door ons gemaakte invorderingskosten en vervolgens ter voldoening van de oudste openstaande facturen.
5. Indien betaling niet op de overeengekomen wijze heeft plaatsgevonden, is de Deelnemer en/of Wederpartij van rechtswege in verzuim en vanaf dat moment een rente van 12% per (gedeelte van een) maand verschuldigd over het nog openstaande bedrag.
6. In geval van niet tijdige betaling door de Deelnemer en/of Wederpartij zal Euroforum de daardoor te maken of veroorzaakte gerechtelijke en buitengerechtelijke kosten van de wederpartij vorderen. De buitengerechtelijke kosten worden gesteld op 15% van het te vorderen bedrag.

Artikel 5: Eigendomsvoorbehoud

1. Alle door Euroforum aan de Deelnemer en/of Wederpartij (over te dragen) zaken blijven in eigendom van Euroforum, maar voor rekening en risico van de Deelnemer en/of Wederpartij, totdat alle verschuldigde bedragen krachtens de overeenkomst, alsmede eventuele vorderingen wegens het tekortkomen in de nakoming, waaronder tevens begrepen de in rekening gebrachte rente en kosten van de invordering, volledig door de Deelnemer en/of Wederpartij zijn voldaan.
2. De Deelnemer en/of Wederpartij en of diens hulppersonen wenden alle daartoe benodigde zorg aan en nemen alle daartoe noodzakelijke maatregelen om de in het vorige lid bedoelde zaken af te scheiden en afgescheiden te houden van overige bij de Deelnemer en/of Wederpartij en/of hulppersonen aanwezige zaken. De in het eerste lid genoemde zaken worden daartoe afzonderlijk opgeslagen of gemerkt, op een zodanige manier dat deze voor derden duidelijk zijn te herkennen als eigendom van Euroforum. Deelnemer en/of Wederpartij zijn gehouden om aan Euroforum of een door Euroforum aangewezen gevolmachtigde te allen tijde vrije toegang te verlenen tot de ruimten waarin de door Euroforum geleverde zaken zich bevinden.
3. Zolang het eigendom van de geleverde zaken niet op de Deelnemer en/of Wederpartij is overgegaan, is het niet toegestaan de zaken te verwerken, te vervreemden, te verpanden of anderszins te bezwaren.
4. De Wederpartij is gehouden om derden die zich op de door Euroforum geleverde zaken willen verhalen te wijzen op het eigendomsvoorbehoud van Euroforum. Voorts is de Wederpartij verplicht Euroforum onverwijld op de hoogte te stellen.
5. Indien de Wederpartij tekortschiet in de nakoming van diens verplichtingen of, indien Euroforum een goede grond heeft te vrezen dat de Wederpartij in diens verplichten tekort zal schieten, is Euroforum gerechtigd het gemaakte eigendomsvoorbehoud te effectueren.
6. Indien Euroforum een beroep doet op het eigendomsvoorbehoud, dan is de Wederpartij verplicht om desgevraagd onmiddellijk en kosteloos de geleverde zaken in de feitelijke macht van Euroforum te brengen.

Artikel 6: Intellectueel Eigendom

1. Alle rechten van intellectueel of industrieel eigendom op alle krachtens de overeenkomst ontwikkelde of ter beschikking gestelde tekeningen, mallen, litho's ontwerpen, schetsen, modellen, documenten en zaken, alsmede voorbereid materiaal daarvan tezamen berusten bij Euroforum en diens licentiegevers.
2. Wederpartij verkrijgt uitsluitend de gebruiksrechten en bevoegdheden die bij deze voorwaarden of anderszins uitdrukkelijk aan u worden toegekend. Het eigendom van de in het eerste lid genoemde informatie blijft onvervreemdbaar bij Euroforum doch voor rekening en risico van de Wederpartij. Het bepaalde in artikel 5 van deze algemene voorwaarden is eveneens van toepassing ten aanzien van dit artikel.
3. Het is niet toegestaan het intellectueel eigendom ter beschikking te stellen aan derden, te verveelvoudigen of daarvan kopieën te (laten) vervaardigen, tenzij en voorzover Euroforum daarvoor voorafgaand schriftelijk toestemming heeft verleend.
4. De Wederpartij is verplicht tot geheimhouding van alle door Euroforum aan de Wederpartij ter beschikking gestelde informatie, tenzij en voorzover Euroforum schriftelijke toestemming tot openbaarmaking heeft verleend.

Artikel 7: Inbreuk op rechten van derden

1. Indien door de bevoegde rechter in een rechtsgeding tegen Euroforum onherroepelijk wordt vastgesteld dat een door Euroforum geleverde zaak inbreuk maakt op een recht van intellectuele of industriële eigendom van een derde, zal Euroforum te harer keuze de betrokken zaak vervangen voor een product dat geen inbreuk maakt op het betreffende recht, een gebruiksrecht ter zake verwerven of de door de Wederpartij betaalde prijs terugbetalen, verminderd met een eventuele afschrijving.
2. Ingeval van vervanging of terugbetaling komt Euroforum het recht toe de oorspronkelijk geleverde zaak terug te nemen.
3. Op Euroforum rust met betrekking tot enig inbreuk op rechten van derden geen andere verplichting dan de in het eerste lid vermelde vervanging-, verwerving-, of terugbetalingsverplichting.
4. Ingeval Euroforum een opdracht uitvoert naar ontwerp, tekeningen, specificaties of aanwijzingen, door of namens de wederpartij verstrekt dan garandeert de Wederpartij dat het gebruik daarvan niet in strijd is met wettelijke voorschriften of beschermende rechten van derden en vrijwaart de Wederpartij Euroforum van alle daarmee in verband houdende gestelde inbreuken op rechten van intellectueel of industrieel eigendom van derden.

Artikel 8: Aansprakelijkheid

1. Euroforum is uitsluitend aansprakelijk voor directe schade, veroorzaakt door het geven van Bijeenkomsten, met dien verstande dat deze aansprakelijkheid is beperkt tot een bedrag van maximaal € 500.000,- per gebeurtenis vermeerderd met het eigen risico dat Euroforum in verband met die verzekering draagt. In ieder geval gaat de aansprakelijkheid het door de verzekering eventueel uit te keren maximale bedrag niet te boven.
2. Indien als gevolg van een gebeurtenis genoemd in artikel 8 onder lid 1 meer dan één vordering ontstaat en de gezamenlijke vorderingen de in datzelfde lid gestelde maximum overschrijdt, is Euroforum slechts verplicht de vorderingen naar evenredigheid te voldoen. Euroforum is slechts aansprakelijk tot het in artikel 8 onder lid 1 genoemde maximum van in totaal € 750.000,- per kalenderjaar. In ieder geval gaat de aansprakelijkheid het door de verzekering eventueel uit te keren maximum bedrag niet te boven.
3. Indien, om welke reden dan ook, geen uitkering door de hiervoor genoemde verzekering plaatsvindt, is de aansprakelijkheid van Euroforum, uit welke hoofde dan ook, te allen tijde beperkt tot de op dat moment door Euroforum bij de Deelnemer en/of Wederpartij in rekening gebrachte en betaalde facturen, verbonden aan de desbetreffende overeenkomst.
4. Onder directe schade wordt in de zin van dit artikel uitsluitend verstaan:
 - a. De redelijke kosten die de Deelnemer en/of Wederpartij heeft gemaakt in het kader van de tussen partijen gesloten overeenkomst;
 - b. De redelijke kosten ter vaststelling van de oorzaak en omvang van de schade, mits de Wederpartij Euroforum op voorhand op de hoogte stelt van de wijze en noodzaak daarvan;
 - c. De redelijke kosten gemaakt ter voorkoming of beperking van schade, voor zover de Deelnemer en/of Wederpartij kan aantonen dat deze kosten daadwerkelijk hebben geleid tot een beperking van de directe schade in de zin van dit artikel.
5. In geen geval is Euroforum aansprakelijk voor indirecte schade, daaronder begrepen, winstderving ten gevolge van het niet of niet naar behoren geven van de Bijeenkomst, het verlenen van andere diensten of enigerlei andere gevolgschade.
6. De totale aansprakelijkheid van Euroforum voor schade door dood of lichamelijk letsel of voor materiële beschadiging van goederen zal in geen geval meer bedragen dan het bedrag dat door de verzekering van Euroforum wordt uitgekeerd. Ten aanzien van aansprakelijkheid voor materiële beschadiging van goederen van derden geldt dat de aansprakelijkheid in geen geval meer zal bedragen dan het bedrag dat onder de verzekering van Euroforum wordt uitgekeerd.
7. Schadeclaims moeten onverwijld, doch in elk geval binnen één (1) jaar na afloop van de Bijeenkomst bij Euroforum schriftelijk zijn gemeld.

Artikel 9: Overmacht

1. Onder overmacht wordt verstaan: elke van de wil van partijen onafhankelijke c.q. onvoorzienbare omstandigheid waardoor nakoming van de overeenkomst redelijkerwijs door de andere partij niet meer kan worden verlangd, bijvoorbeeld in het geval van brand, overstroming, werkstaking, epidemieën, (burger)oorlog, overheidsmaatregelen, niet (tijdig) beschikbaar zijn van vergunningen, handelsembargo's, elektriciteitsuitval, bedrijfsstoring, wanprestatie bij of vertraging aan de zijde van toeleveranciers van Euroforum en de door Euroforum ingeschakelde derden dan wel hun personeel en het bij Euroforum niet (tijdig) of onvoldoende beschikbaar zijn van materialen, transport, brandstoffen, energie, en arbeidskracht.
2. Indien naar oordeel van Euroforum de overmacht van tijdelijke aard zal zijn, heeft Euroforum het recht de uitvoering van de overeenkomst op te schorten, totdat de omstandigheden die de overmacht opleveren zich niet meer voordoen.
3. Is naar oordeel van Euroforum de overmacht van blijvende aard, of is de uitvoering van de overeenkomst langer dan 3 maanden opgeschort of zodra zeker is dat deze tenminste drie maanden zal duren dan kan elk van de partijen bij aangetekend schrijven vorderen dat de overeenkomst hetzij aan de omstandigheden wordt aangepast, hetzij met onmiddellijke ingang van het betreffende deel wordt ontbonden, zonder dat partijen daarbij over en weer tot schadevergoeding gehouden zijn.
4. Euroforum is steeds gerechtigd betaling te vorderen van de prestaties die reeds bij de uitvoering van desbetreffende overeenkomst zijn verricht voordat de overmachtsomstandigheid zich voordeed.
5. De partij die meent in overmacht te verkeren, dient de andere partij daarvan onmiddellijk in kennis te stellen.

Artikel 10: Ontbinding

1. Indien één der partijen:
 - a. In staat van faillissement wordt verklaard, tot boedelafstand overgaat, een verzoek tot surseance van betaling indient dan wel dat beslag wordt gelegd op het geheel of gedeelte van haar eigendommen;
 - b. (Bij natuurlijk persoon) komt te overlijden of onder curatele wordt gesteld;
 - c. Op grond van de wet of overeenkomst haar verplichtingen niet dan wel niet behoorlijk nakomt;
 - d. Een factuurbedrag niet voldoet binnen de gestelde termijn dan wel niet voldoet aan het verzoek van Euroforum tot vooruitbetaling, contante betaling of op verzoek geen zekerheid stelt,
 - e. Overgaat tot staking van het bedrijf;hebben partijen het recht de overeenkomst door middel van een schriftelijke verklaring geheel of gedeeltelijk te ontbinden zonder dat enige rechterlijke tussenkomst of ingebrekestelling is vereist onverminderd het recht op vergoeding van alle directe, indirecte en gevolgschade, inclusief gederfde winst en onverminderd alle andere toekomstige rechten.

Artikel 11: Verandering van datum

1. Mocht een Deelnemer en/of Wederpartij verhinderd zijn op de ingeschreven datum van de Bijeenkomst dan kan de Deelnemer en/of Wederpartij schriftelijk verzoeken om de Deelnemer en/of Wederpartij deel te laten nemen aan een andere bijeenkomst op een andere datum.
2. De Deelnemer en/of Wederpartij kan tot 1 maand voor de aanvangsdatum van de Bijeenkomst kosteloos veranderen van datum of annuleren overeenkomstig artikel 13 van deze algemene voorwaarden.
3. Indien de Deelnemer en/of Wederpartij binnen 1 maand voor de aanvangsdatum van de Bijeenkomst op een andere datum wenst deel te nemen dan krijgt de Deelnemer en/of Wederpartij een tegoedbon ter waarde van de prijs van de Bijeenkomst (onder aftrek van € 150,- voor overboekingskosten) exclusief BTW en kan de Deelnemer en/of Wederpartij zich met deze tegoedbon inschrijven op een andere Bijeenkomst. De Deelnemer en/of Wederpartij heeft geen recht op restitutie.
4. Indien de Deelnemer en/of Wederpartij het inschrijfgeld nog niet betaald heeft op het moment dat de Deelnemer en/of Wederpartij het verzoek doet om een Bijeenkomst op een andere datum te volgen dan blijft de Deelnemer en/of Wederpartij het inschrijfgeld verschuldigd en ontvangt de Deelnemer en/of Wederpartij na betaling een tegoedbon ter waarde van het Inschrijfgeld (onder aftrek van de eventuele overboekingskosten).
5. Bijeenkomsten vinden slechts doorgang onder het voorbehoud van voldoende deelnemers. Indien door Euroforum wordt vastgesteld dat er onvoldoende deelnemers zijn dan is Euroforum gerechtigd de overeenkomst te annuleren. In dit geval ontvangt de Deelnemer en/of Wederpartij uiterlijk één (1) week voor de aanvangsdatum van de Bijeenkomst een bericht en zal het reeds betaalde Inschrijfgeld op verzoek van de Deelnemer en/of Wederpartij gerestitueerd worden of worden verrekend met eventuele openstaande facturen.

Artikel 12: Indeplaatsstelling

Het is toegestaan dat de Deelnemer en/of Wederpartij zich laat vervangen, mits de Deelnemer en/of Wederpartij in het bezit is van een geldig toegang- en/of inschrijfbewijs en dit schriftelijk vooraf door Euroforum is bevestigd.

Artikel 13: Annulering

1. Annulering van de aanmelding dient schriftelijk per brief of per e-mailbericht te geschieden.
2. Annulering is kosteloos tot 1 maand voor aanvangsdatum van de Bijeenkomst.
3. Indien de Deelnemer en/of Wederpartij annuleert binnen één (1) maand voor aanvangsdatum van de Bijeenkomst dan wordt aan de Deelnemer en/of de Wederpartij een tegoedbon ter waarde van het Inschrijfgeld (onder aftrek van € 150,- voor annuleringskosten) exclusief BTW verstrekt. De Deelnemer en/of Wederpartij kan deze tegoedbon conform artikel 14 van deze algemene voorwaarden gebruiken om aan een andere Bijeenkomst deel te nemen.
4. Indien de Deelnemer en/of Wederpartij het Inschrijfgeld op het moment van annulering nog niet betaald heeft en er is sprake van een situatie zoals omschreven in artikel 13 lid 3, dan is de Deelnemer en/of Wederpartij het Inschrijfgeld verschuldigd en ontvangt de Deelnemer en/of Wederpartij na betaling een tegoedbon ter waarde van het Inschrijfgeld (onder aftrek van de annuleringskosten).
5. Voor abonnementen geldt naast de toepassing van deze algemene voorwaarden tevens hetgeen bepaald in artikel 18.

Artikel 14: Tegoedbon

1. De tegoedbon is één jaar na uitgifte door Euroforum geldig. Daarna vervalt de tegoedbon.
2. De tegoedbon wordt op naam verstrekt en kan alleen door de Deelnemer en/of Wederpartij worden gebruikt. Overdragen en derden is niet mogelijk.
3. Indien de Deelnemer en/of Wederpartij aan een Bijeenkomst wenst deel te nemen waarvoor een lager Inschrijfgeld wordt gehanteerd dan de waarde van de eerder verstrekte tegoedbon, dan wordt dit verschil aan de Deelnemer en/of Wederpartij niet geretourneerd en ontvangt deze voor het resterende bedrag wederom een tegoedbon.
4. Indien de Deelnemer en/of Wederpartij aan een Bijeenkomst wil deelnemen met een hoger Inschrijfgeld dan de waarde van de tegoedbon, ontvangt de Deelnemer en/of Wederpartij een aanvullende factuur voor het verschil tussen de waarde van de tegoedbon en het inschrijfgeld van de Bijeenkomst. Op deze factuur zijn de voorwaarden van artikel 4 onverkort van toepassing.

Artikel 15: Persoonsgegevens

1. De door Euroforum verzamelde persoonsgegevens worden in het kader van de uitvoering van de overeenkomst door Euroforum verwerkt en worden gebruikt voor de efficiënte inrichting van Euroforum in het kader van marktonderzoek en marktbenadering.
2. De Deelnemer en/of Wederpartij hebben een inzage- en correctierecht met betrekking tot de over hen opgenomen persoonsgegevens. Daarnaast is de Deelnemer en/of Wederpartij gerechtigd bezwaar te maken bij Euroforum tegen het verwerken van zijn of haar persoonsgegevens.

Artikel 16: Sponsoring, Promotie, Standverhuur

1. De Wederpartij draagt er zorg voor dat Euroforum tijdig voor de aanvang van het congres beschikt over de gegevens en/of materialen en/of logo's, waarvan Euroforum heeft aangegeven dat zij die nodig acht promoties, sponsorship en/of andere activiteiten tijdens het congres mogelijk te maken.
2. In geval van het promoties, sponsorship, huren van standruimte en/of andere activiteiten tijdens een congres van Euroforum en/of onze opdrachtgever, gelden bovendien de volgende bepalingen:
 - a. Aan de inschrijving kunnen geen rechten worden ontleend. Euroforum is gerechtigd aanvragen te weigeren. Tevens is Euroforum steeds gerechtigd een inschrijving niet in behandeling te nemen, alsmede minder standruimte vast te stellen dan waarvoor is ingeschreven, zonder dat de Wederpartij aanspraak kan maken op vergoeding van enigerlei schade.
 - b. Met uitzondering op artikel 13 van deze algemene voorwaarden kunnen Inschrijvingen binnen 8 weken voor aanvangsdatum van een congres niet meer geannuleerd worden.
 - c. Met uitzondering op artikel 13 van deze overeenkomst geldt voor de annulering van promoties, sponsorship, huur van een standruimte en/of andere activiteiten alleen mogelijk indien aan de volgende voorwaarden wordt voldaan:
 - Wanneer de Wederpartij annuleert tot 18 weken voor de aanvangsdatum van het congres wordt 25% van de totaal overeengekomen prijs in rekening gebracht.
 - Wanneer de Wederpartij annuleert tussen 18 weken en 8 weken voor aanvangsdatum van het congres wordt 50% van de totaal overeengekomen prijs in rekening gebracht.
 - Annulering binnen 8 weken voor aanvangsdatum is niet mogelijk en zal altijd leiden tot een betalingsverplichting van het volledige bedrag.
 - Annulering dient schriftelijk en aangetekend plaats te vinden.
3. Euroforum behoudt zich te allen tijde het recht voor om de datum en locatie van het congres te wijzigen of het congres niet door te laten gaan. In die gevallen kunt u geen aanspraak maken op vergoeding van enigerlei schade.
4. Indien een congres niet door gaat worden de standinschrijvingen en verstrekte standruimte als vervallen beschouwd en zullen betalingen met betrekking tot de huur van de standruimte gerestitueerd worden.
5. Euroforum kan in overleg met de Wederpartij de reeds toegewezen standruimte wijzigen, dan wel een reeds verleende vaststelling intrekken, indien dit om organisatorische redenen noodzakelijk is. De Wederpartij kan in dergelijke gevallen geen recht doen gelden op vergoeding van schade, in welke vorm of door welke oorzaak die ook mocht zijn ontstaan.
6. De inrichting en ontruiming van een stand moet geschieden in overleg met Euroforum. Euroforum is te allen tijde gerechtigd hierbij bindende voorschriften te geven. Euroforum is, zonder daartoe tot enige schadevergoeding verplicht te zijn, gerechtigd om zaken en diensten die niet vermeld zijn op het inschrijvingsformulier en die Euroforum niet toelaatbaar acht te weigeren respectievelijk terstond van het congres te doen (laten) verwijderen.
7. Een half uur voor ontvangst van de deelnemers moet de stand gereed zijn. Direct na afloop van het congres dient de stand te worden ontruimd.
8. Onverminderd hetgeen bepaald in artikel 8 van deze algemene voorwaarden geldt voor congressen het volgende:
 - a. Zaken die zich bevinden in het tentoonstellingsgebouwen of bijbehorende terreinen zijn voor eigen rekening en risico van de Wederpartij. Euroforum is niet gehouden deze te verzekeren.
 - b. Euroforum is niet aansprakelijk voor enige schade, uit welke oorzaak dan ook, ontstaan aan zaken of personen als gevolg of in verband met het deelnemen aan een door Euroforum georganiseerd congres.
 - c. Euroforum is tevens niet aansprakelijk voor schade van derden veroorzaakt door het gebruik van de stand door de Wederpartij, diens personeel of diens hulppersonen.
 - d. De Wederpartij is zelf aansprakelijk voor en dient verplicht verzekerd te zijn tegen alle schade, die door toedoen of nalatigheid van de Wederpartij, diens personeel, of diens hulppersonen, op welke wijze ook, aan zaken van en/of personen werkzaam bij of in opdracht van ons. Op verzoek van Euroforum dient de Wederpartij aan te tonen dat deze voldoende verzekerd is.
 - e. Euroforum wordt door deelname aan het congres door de Wederpartij gevrijwaard van alle aanspraken van derden op schadevergoeding als bedoeld in dit artikel.
9. Euroforum is niet verantwoordelijk voor het aantal deelnemers aan het congres en is niet aansprakelijk voor welke schade ook in geval van een tegenvallend aantal bezoekers.
10. In alle gevallen, waarin de overeenkomst en deze van toepassingen zijnde algemene voorwaarden niet voorzien, beslist Euroforum als organisator van het congres.

Artikel 17: In-company bijeenkomst

1. Indien Euroforum een In-company bijeenkomst verzorgd zijn daarop de volgende aanvullende bepalingen van toepassing:
 - a. Annulering dient schriftelijk per brief of emailbericht te geschieden.
 - b. Met uitzondering op artikel 13 van deze algemene voorwaarden geldt dat bij een annulering van in-company bijeenkomst één (1) maand voor de datum van de bijeenkomst 40% van de overeengekomen prijs is verschuldigd.
 - c. Bij annulering tussen 1 maand en 2 weken voor de datum van de bijeenkomst is 80% van de overeengekomen prijs verschuldigd.
 - d. Bij annulering binnen 2 weken voor de datum van de bijeenkomst is 100% verschuldigd aan Euroforum
2. De datum van de in-company bijeenkomst kan gewijzigd worden. Hetgeen bepaald onder lid 1 van dit artikel blijft daarbij onverkort van toepassing.
3. Euroforum heeft te allen tijde het recht om de datum van de overeenkomst te wijzigen zonder dat daartoe enige verplichting tot schadevergoeding bestaat.

Artikel 18: Abonnementen

1. Indien Euroforum een overeenkomst sluit met betrekking tot een Abonnement zijn deze algemene voorwaarden van toepassing waarbij bij Bijeenkomst 'Abonnement' gelezen dient te worden.
2. Op abonnementen zijn de volgende specifieke voorwaarden aanvullend van toepassing:
 - a. De betaling dient voor aanvang van de abonnementsperiode te zijn voldaan. Bij niet tijdige betaling wordt het Abonnement stopgezet en ontslaat de Deelnemer en/of Wederpartij niet van enige betalingsverplichting jegens Euroforum.
 - b. Opzegging van het abonnement dient te alle tijde schriftelijk te geschieden (per email of brief), doch uiterlijk twee (2) maanden voor aanvang van de nieuwe abonnementsperiode. Indien niet (tijdig) is opgezegd wordt het Abonnement automatisch verlengd conform de oorspronkelijk overeengekomen periode.

Artikel 19: Toepasselijk recht

1. Alle geschillen, voortvloeiend uit of verband houdende met een aanbieding, opdracht, overeenkomst of verbintenis waarop deze voorwaarden van toepassing zijn, zullen in eerste aanleg uitsluitend worden beslecht door de absoluut bevoegde rechter van de rechtbank Oost-Brabant.
2. Op deze algemene voorwaarden is Nederlands recht van toepassing.

Privacy Statement

Euroforum respecteert de privacy van alle bezoekers van deze website. De gegevens die u op deze site achterlaat worden zorgvuldig en vertrouwelijk behandeld. De gegevens worden opgenomen in een database en kunnen worden gebruikt voor marketingdoeleinden van Euroforum en de aan haar gelieerde ondernemingen*. Deze database is aangemeld bij het College Bescherming Persoonsgegevens.

Uw NAW-gegevens kunnen eventueel ook verstrekt worden aan derden voor het doen van interessante aanbiedingen. Wenst u niet dat uw gegevens door derden worden gebruikt, dan kunt u contact opnemen met onze afdeling klantenservice: klant@euroforum.nl

Het kan zijn dat u ook via e-mail door ons op de hoogte wordt gehouden van bijeenkomsten en ontwikkelingen op uw vakgebied. We houden hierbij rekening met de eisen die de nieuwe telecomwet hieraan stelt. Mocht u geen e-mailings meer willen ontvangen, dan kunt u zich op elk gewenst moment hiervoor afmelden via de link onderaan elke mailing. E-mailadressen worden niet aan derden ter beschikking gesteld.

Heeft u een vraag hierover, neem dan contact op met onze klantenservice.

** Euroforum hanteert ook de volgende merknamen: European Business Studies, Studiecentrum voor Bedrijf en Overheid, Secretary Management Institute, Fiscaal Up To Date en het Nederlands Instituut voor de Bouw*

Disclaimer

De tekst op deze website is met grote zorg samengesteld en mag op generlei wijze worden overgenomen of gekopieerd. Wij aanvaarden geen aansprakelijkheid voor informatie die onvolledig of onjuist is opgenomen.

Bron

EF: <http://www.euroforum.nl/klantenservice/>
SBO: <http://www.sbo.nl/klantenservice/>
SMI: <http://www.secretary.nl/klantenservice/>
NIB: <http://www.bouw-instituut.nl/klantenservice/>

Privacy

Euroforum* en de aan haar gelieerde ondernemingen** respecteert de privacy van alle bezoekers van haar website. Onze werknemers zijn verplicht om de vertrouwelijkheid van uw gegevens te respecteren. De gegevens die u op deze site achterlaat worden zorgvuldig en vertrouwelijk behandeld, in overeenstemming met geldende wet- en regelgeving.

Lees onderstaand hoe wij met uw gegevens omgaan.

Euroforum is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze privacy verklaring

Waarvoor verwerken wij persoonsgegevens

Euroforum verzamelt persoonsgegevens voor verschillende doeleinden.

- Wanneer u producten en/of diensten van Euroforum* afneemt. Dit kan via onze website, telefonisch en per email.
- Wanneer u contact heeft met Euroforum*. Dit contact kan telefonisch zijn, maar hieronder verstaan wij ook indien u ons via e-mail benadert, het contactformulier invult, gebruik maakt van de chatfunctie, meedoet aan enquêtes, prijsvragen of (panel)onderzoeken, gebruik maakt van onze (mobiele) websites, inclusief apps, inlogt op uw account, u aanmeldt voor nieuwsbrieven of ons via social media benadert.
- Voor de uitvoering van de overeenkomsten zoals bevestiging van deelname aan onze congressen en opleidingen, of afname van abonnementen en de praktische zaken rondom deelname aan een opleiding zoals de online leeromgeving. Voor de registratie van deelname maken wij gebruik van een online registratiesysteem.
- Om u op de hoogte te houden van (nieuwe) bijeenkomsten en ontwikkelingen op uw vakgebied, rechtstreeks maar ook door campagnes via social media. Euroforum houdt hierbij rekening met de voorkeuren van afgenomen producten en op basis van met uw toestemming vastgelegd gebruik.

Email

Euroforum en de haar gelieerde ondernemingen* hebben elk eigen nieuwsbrieven. Wanneer u toestemming heeft gegeven voor het verzenden van een nieuwsbrief dan wordt deze toegezonden. U kunt uw toestemming altijd intrekken door u af te melden voor de betreffende nieuwsbrief in de afmeldlink.

Uw emailadres wordt verder gebruikt voor het toesturen van informatie over (nieuwe) producten en diensten indien u daarvoor toestemming heeft gegeven. Wij gebruiken hiervoor een e-mail marketing tool. De toestemming kunt u altijd intrekken door gebruik te maken van de afmeldlink in het toegezonden emailbericht, via onze klantenservice 04  of via klant@euroforum.nl. Uw emailadres wordt niet aan derden ter beschikking gesteld.

Recht van Verzet

Indien u in het geheel geen prijs stelt op informatie over (nieuwe) bijeenkomsten en ontwikkelingen op uw vakgebied, kunt u uw toestemming altijd intrekken door gebruik te maken van de afmeldlink in het toegezonden e-mailbericht, via onze klantenservice 04  of via klant@euroforum.nl.

Gegevens inzien, aanpassen of verwijderen

U heeft het recht om uw persoonsgegevens in te zien, te corrigeren, te verwijderen of op te vragen. U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens doen. Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan,

vragen wij u een kopie van uw identiteitsbewijs met het verzoek mee te sturen. We reageren zo snel mogelijk, maar binnen vier weken, op uw verzoek.

Cookies

Euroforum* maakt gebruik van cookies. Cookies zijn kleine tekstbestandjes die op uw pc, tablet of mobiele telefoon worden geplaatst. Deze cookies worden gebruikt om de websites van Euroforum* te helpen analyseren hoe gebruikers de site gebruiken. De door het cookie gegenereerde informatie over uw gebruik van de website (met inbegrip van uw IP-adres) kan niet worden herleid naar een pc of individu.

Euroforum* maakt gebruik van functionele- en tracking cookies, alsmede cookies van derden; t.w. Google analytics, Facebook, Adwords, Zopim, Clang en LinkedIn.

Deze worden gebruikt voor het onthouden van loginnaam, instellingen of koppelen van een browser aan tijdelijke variabelen op de server, of voor het maken van een profiel van de bezoeker, zoals waar de bezoeker vandaan komt en welke pagina's bezocht zijn.

U kunt het gebruik van cookies weigeren door in uw browser de daarvoor geëigende instellingen te kiezen. Door gebruik te maken van deze website geeft u toestemming voor het verwerken van de informatie door Google.

Delen van gegevens met derden

Euroforum BV verkoopt uw gegevens niet aan derden en verstrekt deze uitsluitend indien dit nodig is voor de uitvoering van onze overeenkomst met u of om te voldoen aan een wettelijke verplichting. Met bedrijven die uw gegevens verwerken in onze opdracht, sluiten wij een bewerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. Euroforum BV blijft verantwoordelijk voor deze verwerkingen.

Beveiliging en zorgvuldige omgang van persoonsgegevens

Wij maken gebruik van strikte veiligheidsprocedures onder meer om te voorkomen dat onbevoegden toegang krijgen tot onze persoonsgegevens. Exports worden gelogd. Voor het interne netwerk wordt een beveiligde Client/server verbinding gebruikt en voor de webformulieren https. Onze wachtwoorden zijn versleuteld, onze data zijn opgeslagen in Europa en deze worden niet verzonden naar landen buiten Europa.

Daarnaast hanteren wij grote zorgvuldigheid tav onze persoonsgegevens. De gegevens zijn alleen toegankelijk voor medewerkers die expliciet toegang tot de systemen hebben gekregen. Tevens hebben wij met al onze bewerkers bewerkingsovereenkomsten gesloten. Indien u de indruk heeft dat uw gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact met ons op.

Wijzigingen Privacyverklaring

Wij behouden ons het recht voor om wijzigingen aan te brengen in deze verklaring. Het verdient aanbeveling om deze verklaring geregeld te raadplegen, zodat u van deze wijzigingen op de hoogte bent.

*Euroforum BV, Emmasingel 29-17, 5611 AZ Eindhoven, 040-2974974

** Gelieerde ondernemingen Euroforum: Studiecentrum voor Bedrijf en Overheid, Secretary Management Institute, Fiscaal up to Date en het Nederlands Instituut voor de Bouw

Uw privacy

De Nationale ombudsman verwerkt voor het uitvoeren van zijn wettelijke taken en zijn bedrijfsvoering persoonsgegevens en vindt het belangrijk dat met deze persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk worden behandeld. Wij verwerken uw persoonsgegevens in overeenstemming met de geldende wet- en regelgeving. Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming van kracht.

Wat doen wij met uw persoonsgegevens?

Dient u een klacht bij ons in, dan vragen we u om uw persoonsgegevens. Deze gegevens hebben wij nodig om uw klacht te kunnen behandelen. Verstrekt u de gegevens niet, dan kunnen wij uw klacht niet behandelen.

Daarnaast verwerken wij persoonsgegevens voor dienstverlenende taken, bijvoorbeeld als u een brochure of publicatie van ons wilt ontvangen. Ook verwerken wij uw persoonsgegevens als u bijvoorbeeld solliciteert op een functie bij de Nationale ombudsman. Wij gebruiken uw persoonsgegevens alleen voor het doel waarvoor u ze verstrekt.

Delen wij uw gegevens met anderen?

De behandeling van uw klacht kan met zich meebrengen dat de Nationale ombudsman gegevens, inclusief persoonsgegevens, deelt met de bij uw klacht betrokken overheidsinstanties. Daarom raden wij u aan alleen die informatie op te sturen die wij nodig hebben voor de behandeling van uw klacht. Bij twijfel kunt u telefonisch contact [<link naar contact>](#) met ons opnemen.

Voor de dienstverlenende taken wisselen wij geen persoonsgegevens uit met andere instanties. Wij gebruiken uw persoonsgegevens nooit voor commerciële of andere doeleinden dan waarvoor ze zijn verstrekt.

Met organisaties die – in opdracht van de Nationale ombudsman – uw gegevens verwerken, sluiten wij een verwerkersovereenkomst. De Nationale ombudsman blijft verantwoordelijk voor de verwerking van uw gegevens.

Hoe lang bewaren wij uw persoonsgegevens?

De Nationale ombudsman bewaart persoonsgegevens niet langer dan noodzakelijk en wettelijk is toegestaan. De Archiefwet 1995 schrijft de bewaartermijnen voor. In zogenaamde selectielijsten is vastgelegd welke informatie de Nationale ombudsman na verloop van tijd vernietigd of blijvend worden bewaard.

Als u bij ons solliciteert en u wordt afgewezen, dan worden uw gegevens 1 maand na afwijzing verwijderd. Wij kunnen uw toestemming vragen om uw gegevens maximaal 1 jaar te bewaren.

Als er voor specifieke gegevens geen wettelijke bewaartermijn is, bewaren wij de gegevens niet langer dan noodzakelijk is voor de dienstverlening.

Uw privacyrechten

U heeft een aantal rechten als de Nationale ombudsman uw persoonsgegevens gebruikt:

- *Recht op informatie:* u heeft het recht om te weten waarom uw persoonsgegevens nodig zijn, wat ermee gebeurt en hoelang ze worden bewaard.
- *Recht op inzage:* u heeft het recht op inzage in uw persoonsgegevens die bij ons bekend zijn.
- *Recht op rectificatie:* u heeft het recht om ons te vragen uw persoonsgegevens aan te vullen of te corrigeren wanneer de persoonsgegevens die wij van u hebben onjuist zijn.

Het is niet mogelijk na afloop van de klachtbehandeling te vragen om correctie van gestelde feiten, meningen en conclusies waarmee u het niet eens bent. Wel mag u van ons verwachten dat wij uw schriftelijke mening toevoegen aan uw dossier.

- *Recht op beperking van de verwerking:* u heeft het recht om te vragen dat de verwerking van uw persoonsgegevens tijdelijk wordt stopgezet, bijvoorbeeld omdat u bezwaar heeft gemaakt tegen de verwerking van uw persoonsgegevens en u nog op een antwoord wacht.
- *Recht van bezwaar:* u heeft het recht om – vanwege persoonlijke omstandigheden – bezwaar te maken tegen de verwerking van uw persoonsgegevens. U kunt alleen bezwaar maken als de verwerking van uw persoonsgegevens plaatsvindt op grond van de uitoefening van een publieke taak of als de Nationale ombudsman meent een gerechtvaardigd belang te hebben bij de verwerking van uw persoonsgegevens.
- *Recht op verwijdering en recht om vergeten te worden:* wanneer u toestemming aan ons geeft om uw gegevens te verwerken, dan heeft u het recht om de persoonsgegevens weer te laten verwijderen.

Beperking van uw privacyrechten

Als uw verzoek betrekking heeft op een door u ingediende klacht, dan zijn uw rechten beperkt. De verwerking van persoonsgegevens tijdens de klachtbehandeling berust namelijk niet op toestemming, dus die kunt u ook niet intrekken.

Gebruik maken van uw privacyrechten

Wilt u van één van uw rechten gebruikmaken, dan kunt u schriftelijk of per e-mail een verzoek indienen. Uw verzoek stuurt u naar:

Nationale ombudsman

T.a.v. de functionaris voor de gegevensbescherming

Postbus 93122

2509 AC Den Haag

Het e-mailadres dat u kunt gebruiken is: avg@nationaleombudsman.nl

Wij behandelen uw verzoek in beginsel binnen vier weken na ontvangst. Indien nodig vragen wij hierna nog verdere informatie bij u op.

Heeft u een klacht over het gebruik van uw persoonsgegevens?

Heeft u een klacht over het gebruik van uw persoonsgegevens door de Nationale ombudsman, dan kunt u daarover [contact](#) <link naar contact> met ons opnemen. Ook kunt u daarover een [klacht](#) <link naar webpagina met informatie hoe klacht bij No kan worden ingediend> bij ons indienen.

Komt u er samen met ons niet uit, dan kunt u uw klacht indienen bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op het gebruik van persoonsgegevens.

Functionaris voor de gegevensbescherming

De Nationale ombudsman heeft een functionaris voor de gegevensbescherming. Deze ziet erop toe dat wij persoonsgegevens verwerken volgens de wet. De functionaris voor de gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens. U kunt in contact komen met de functionaris voor de gegevensbescherming via het e-mailadres: avg@nationaleombudsman.nl

Hoe gaan online partijen om met uw privacy?

Wij gaan vertrouwelijk om met de persoonlijke informatie die u ons geeft. Komt u via links op onze website terecht op andere websites, zoals Facebook, Twitter en WhatsApp? Dan gelden daar de regels van die partijen voor de omgang met uw persoonlijke informatie en privacy. Wij raden u dan ook aan hun privacybepalingen goed door te lezen.

Anonimiseren van persoonsgegevens in publicaties

De Nationale ombudsman publiceert zijn rapporten op deze website. Hierbij worden de rapporten geanonimiseerd. Dit gebeurt op zo'n manier dat zaken niet meer zijn te herleiden tot een individueel persoon. Als u van mening bent dat dit in uw geval niet zorgvuldig is, dan kunt u een mail sturen naar de functionaris gegevensbescherming: avg@nationaleombudsman.nl

Wat doen wij met cookies?

Deze website maakt gebruik van cookies. De cookies gebruiken wij om de website beter te laten functioneren en om het bezoek aan de website te monitoren. We gebruiken deze gegevens niet op individueel persoons- of computerniveau. De gegevens zijn daarom niet te herleiden tot een bepaalde computer of persoon. Zie verder ons [cookiebeleid](#).

Wijzigingen

Wij behouden ons het recht voor om wijzigingen aan te brengen in deze privacyverklaring en ons cookiebeleid. De actuele versie vindt u altijd op deze pagina.

Van: [redacted]
Verstuurd: Mon, 28 May 2018 12:00:35 +0200
Aan: [redacted]
Onderwerp: FW: Aanmelding Functionaris voor de gegevensbescherming

Van: Autoriteit Persoonsgegevens [redacted]@autoriteitpersoonsgegevens.nl]
Verzonden: maandag 28 mei 2018 10:42
Aan: [redacted]
Onderwerp: Aanmelding Functionaris voor de gegevensbescherming

Geachte heer/mevrouw,

U bent aangemeld als functionaris voor de gegevensbescherming (FG) voor de organisatie de Nationale ombudsman. Van harte gefeliciteerd met deze aanstelling. Het aan u toegekende FG-nummer is [redacted]. Als FG heeft u een belangrijke en verantwoordelijke functie. U ziet erop toe dat de Algemene Verordening Gegevensbescherming binnen uw organisatie goed wordt toegepast en nageleefd.

De Autoriteit Persoonsgegevens publiceert voorlichtingsmateriaal, beleidsregels en vraag-en-antwoordlijsten op haar website. Zie voor meer informatie <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming>.

U kunt ook meer informatie krijgen via het Nederlands Genootschap voor de Functionaris voor de Gegevensbescherming (het NGFG). Meer informatie over het NGFG vindt u op www.ngfg.nl.

Wilt u een signaal afgeven of een zaak voorleggen waarbij onduidelijkheid bestaat over de norm? Neemt u dan contact met ons op via [redacted]@autoriteitpersoonsgegevens.nl.

Wij wensen u veel succes met uw nieuwe functie.

Met vriendelijke groet,

[redacted]

Directeur Systeemtoezicht, beveiliging en technologie



AUTORITEIT
PERSOONSGEGEVENS

[redacted]@autoriteitpersoonsgegevens.nl
T 070 8888 500 - F 070 8888 501
Prins Clauslaan 60, 2595 AJ Den Haag
Postbus 93374, 2509 AJ Den Haag
autoriteitpersoonsgegevens.nl

Procedure AVG verzoeken

1 Inleiding

1.1 Aanleiding

De Algemene verordening gegevensbescherming (AVG) kent aan betrokkenen een aantal rechten toe, op grond waarvan zij een verzoek kunnen indienen dat betrekking heeft op hun persoonsgegevens. Een overzicht van mogelijke verzoeken is in [bijlage 1](#) opgenomen. Om gehoor te kunnen geven aan dergelijke verzoeken is het van belang dat er een procedure is die houvast biedt bij de afhandeling ervan.

1.2 Reikwijdte

Onderscheid moet worden gemaakt tussen 'interne' en 'externe' betrokkenen. Met de 'interne' betrokkenen worden de medewerkers van de No bedoeld. De 'externe' betrokkenen zijn burgers. De procedure die in dit document wordt beschreven, geldt alléén voor verzoeken van 'externe' betrokkenen.

1.3 Communicatie

Op onze website onder privacy is informatie te vinden over de wijze waarop betrokkenen hun rechten ontleend aan de AVG kunnen uitoefenen.

2 Het verzoek

2.1 Indienen verzoek

Een verzoek van een betrokkene kan via verschillende kanalen worden ontvangen:

- Op onze website worden betrokkenen verzocht een verzoek schriftelijk of per e-mail in te dienen bij de functionaris voor de gegevensbescherming (FG):
Nationale ombudsman
T.a.v. de functionaris voor de gegevensbescherming
Postbus 93122
2509 AC Den Haag
avg@nationaleombudsman.nl
- Een verzoek kan ook via een andere weg of bij een andere medewerker binnenkomen. Bijvoorbeeld via een brief of e-mail in een verzoekdossier.
- Ook telefonisch ingediende verzoeken nemen we in behandeling.

2.2 Verzoek afkomstig van betrokkene

Betrokkene kan slechts een verzoek indienen voor zover het betrekking heeft op zijn/haar eigen gegevens. Dit betekent dat de behandelaar van het verzoek met voldoende zekerheid moet vaststellen dat degene die het verzoek doet daadwerkelijk de betrokkene is.

Het is ook mogelijk om - met een machtiging - een verzoek in te dienen namens iemand anders.

2.3 Identificatie

Wij vragen niet standaard aan iemand om zich te legitimeren door overlegging van zijn/haar legitimatiebewijs. Dit doen we alleen in die gevallen waarin we na de volgende stappen twijfels hebben over de identiteit van degene die het verzoek indient.

- Ga na of de verzoeker en/of intermediair al bij ons bekend is.
- Belt iemand in een lopende zaak overtuig jezelf er dan van dat je met verzoeker of de intermediair zelf te maken hebt.
- Stel zo nodig één of meer controlerende vragen. Informeer b.v. naar het dossiernummer.

Bij twijfel: vraag aan betrokkene om langs te komen en zijn legitimatiebewijs te laten zien. Als dat bezwaarlijk is, bijvoorbeeld omdat betrokkene ver weg woont, ga dan na of de contactpersoon van de betrokken of naburige gemeente bereid is de identificatie voor ons te doen.

2.4 Vertegenwoordiger

Een verzoek kan worden ingediend door een vertegenwoordiger van de betrokkene, bijvoorbeeld een voogd/ouder namens een minderjarig kind of een advocaat namens een cliënt. Om te borgen dat het verzoek daadwerkelijk voor de betrokkene is ingediend, moet de vertegenwoordiger aantonen dat hij/zij bevoegd is de betrokkene te vertegenwoordigen, door een machtiging te overleggen.

2.5 Minderjarigen

Een ouder kan de rechten uit de AVG van zijn/haar kind uitoefenen als die ouder de wettelijke vertegenwoordiger is. Dat is het geval wanneer die ouder het gezag over het kind heeft. Als eraan wordt getwijfeld of de ouder het gezag heeft, kan de ouder gevraagd worden om een recent afschrift van de geboorteakte en een recent uittreksel uit het gezagsregister te overleggen.

2.6 Vreemde talen

Een verzoek kan alleen worden gedaan in de Nederlandse of de Engelse taal. Voor een verzoek in een andere taal moet de betrokkene zelf voor een vertaling zorgen. Het verzoek wordt in het Nederlands of Engels beantwoord.

2.7 Verzoek om inzage o.g.v. de Wob

De Wob is niet van toepassing op de Nationale ombudsman. De Wob is ook niet het juiste juridische kader om persoonsgegevens op te vragen. Wat openbaar is op grond van de Wob is openbaar voor iedereen. Dat is meestal niet de bedoeling van mensen die om inzage in hun eigen persoonsgegevens vragen. Als iemand zich op de Wob beroept om inzage te krijgen in eigen persoonsgegevens moet het verzoek worden gezien als een beroep op artikel 15 van de AVG.

3 Behandeling van het verzoek

3.1 Behandelaar

De ontvangen verzoeken worden behandeld door de medewerker zelf (de dossiereigenaar). Deze betreft een AVG vertegenwoordiger of de functionaris gegevensbescherming bij de behandeling van het verzoek.

Brieven waarmee inhoudelijk wordt gereageerd op een verzoek worden ondertekend door een ambtsdrager. Een weigering moet worden gemotiveerd en de betrokkene moet daarbij worden gewezen op de mogelijkheid een klacht in te dienen bij de Autoriteit Persoonsgegevens.

Complex klaaggedrag

Er zijn verzoekers die bekend zijn met complex klaaggedrag en waarmee 'contactafspraken' zijn gemaakt. In dit soort gevallen gaan e-mails van verzoekers (ook die met AVG verzoeken) naar het groepsadres 'Lastig klaaggedrag'. Achter dit groepsadres zitten de specialisten complex klaaggedrag. Brieven gaan ook naar deze specialisten. Zij bekijken dan eerst of op een brief moet worden gereageerd of niet. Daarna neemt de functionaris gegevensbescherming in overleg met de specialisten de inhoudelijke behandeling van het verzoek over. Wordt besloten om niet te reageren op het verzoek, wordt dit altijd gedaan na overleg met een ambtsdrager. Van de overwegingen die geleid hebben tot dit besluit wordt een notitie gemaakt. Deze notitie wordt opgenomen in het dossier.

3.2 Ontvangstbevestiging

De behandelend medewerker bevestigt de ontvangst van het verzoek (schriftelijk of digitaal) aan de betrokkene. Hiervoor is een standaard tekst opgesteld, opgenomen in [bijlage 2](#). In de ontvangstbevestiging wordt ook vermeld binnen welke termijn het verzoek wordt afgehandeld (uiterste antwoorddatum).

3.3 Reactietermijn

Verzoeken worden in beginsel binnen vier weken na ontvangst behandeld. Indien het gaat om veel verzoeken of complexe verzoeken, dan mogen we twee maanden extra de tijd nemen. Als we daarvan gebruik maken moet de betrokkene hierover binnen een maand na ontvangst van het verzoek worden geïnformeerd.

3.4 Wijze van behandeling

Een verzoek wordt schriftelijk behandeld. Daarbij geldt als uitgangspunt dat bij digitaal ingediende verzoeken de informatie – voor zover mogelijk – ook digitaal wordt verstrekt, tenzij de betrokkene anderszins verzoekt.

Let op! Verstuur geen persoonsgegevens via e-mail tenzij je gebruik kunt maken van 7-Zip.

Op verzoek van betrokkene kan de verzochte informatie ook mondeling worden gegeven, op voorwaarde dat je zeker weet dat het om betrokkene gaat (zie 2.2 t/m 2.5). Leg in het dossier vast welke informatie je precies hebt verstrekt.

De behandeling van een verzoek is kosteloos. Zie verder artikel 12, lid 5, AVG.

3.5 Mogelijkheden ‘preciseringsverzoek’

Als na het in behandeling nemen van het verzoek blijkt dat onvoldoende informatie voorhanden is om adequaat op het verzoek te reageren, kan de behandelend medewerker aanvullende informatie vragen, zoals:

- De duiding van het verzoek (zie [bijlage 1](#)).
- De hoedanigheid van de betrokkene (advocaat, journalist, leverancier, etc.).
- Indien het verzoek een verzoekdossier betreft: of het gaat om een lopende zaak of een afgedane zaak.
- Indien het verzoek geen verzoekdossier betreft: informatie over aard van de betrokkenheid zoals leveranciers, oud-medewerkers, uitzendkrachten, etc.

3.6 Peildatum

Als wordt verzocht om informatie over de verwerking van persoonsgegevens, om inzage in de persoonsgegevens en/of om een kopie van de persoonsgegevens, geldt de datum van ontvangst van het verzoek als peildatum. Dat betekent dat het verzoek betrekking heeft op de persoonsgegevens die de Nationale ombudsman heeft verzameld tot aan de datum van het verzoek. De persoonsgegevens die wij verwerken om aan het verzoek te kunnen voldoen, maken daarvan dus geen onderdeel uit.

3.7 Checklist ter voorbereiding op de beantwoording van het verzoek

Met het oog op een eenduidige en consequente behandeling van verzoeken, en ter voorbereiding op de beantwoording ervan, is een checklist opgesteld. De checklist is opgenomen in [bijlage 3](#).

4 Antwoord (inhoudelijk) op het verzoek

4.1 Geen persoonsgegevens

Het kan zijn dat de Nationale ombudsman geen persoonsgegevens verwerkt van de betrokkene. In dat geval laat de behandelend medewerker de betrokkene weten dat hij/zij niet bekend is bij de Nationale ombudsman en dat er geen persoonsgegevens van hem/haar zijn verwerkt. Hiervoor is een standaard tekst opgesteld ([bijlage 4](#)).

4.2 Geen gevolg geven aan het verzoek / het verzoek wordt beperkt

Slechts in uitzonderlijke situaties kan in zijn geheel of beperkt geen gevolg worden gegeven aan een verzoek. Dit is bijvoorbeeld mogelijk als de betrokkene zich op ons verzoek niet identificeert (art. 11 lid 2 AVG). Het ‘niet kunnen vinden’ van gegevens kan nooit als grond worden aangevoerd. Wanneer geen gevolg aan het verzoek gegeven kan worden, moet de betrokkene daarvan op de hoogte worden gebracht. Dit moet worden gemotiveerd, waarbij ook moet worden gewezen op de mogelijkheid een klacht in te dienen bij de Autoriteit Persoonsgegevens (art. 12 lid 4 AVG).

Beperking van een verzoek is mogelijk als dat op grond van een Europese of nationale wet is voorgeschreven. Voorwaarde is wel dat de beperking niet in strijd is met de inhoud van grondrechten en fundamentele vrijheden en de beperking een noodzakelijke en evenredige maatregel is (art. 23 AVG). Bij verzoeken die betrekking hebben op het primaire proces is eerder dan bij verzoeken aangaande de bedrijfsvoering te verwachten dat aanleiding bestaat het verzoek niet in te willigen of te beperken. De redenen om geen gevolg te geven aan een verzoek of een verzoek te beperken zijn opgenomen in [bijlage 5](#). De standaard tekst voor als het antwoord op het verzoek luidt dat er geen gevolg aan wordt gegeven of dat het verzoek wordt beperkt, is opgenomen in [bijlage 6](#).

4.3 Verzoek inwilligen

Het verzoek wordt ingewilligd, als geen bezwaren bestaan op grond waarvan aan het verzoek van de betrokkene geen gevolg zou moeten worden gegeven of het verzoek beperkt zou moeten worden. Afhankelijk van het verzoek wordt op de volgende wijze aan het verzoek voldaan.

1. Intrekken toestemming verwerking persoonsgegevens

Voor specifieke processen die geen verband houden met het primaire proces kan het zijn dat de betrokkene toestemming heeft gegeven. Denk hierbij aan het versturen van een nieuwsbrief. Wanneer betrokkene de eerder gegeven toestemming intrekt, ontvalt de grond voor verwerking en moet de betrokkene uitgeschreven worden.

2. Informatie over verwerking persoonsgegevens

Wanneer de betrokkene vraagt om uitsluitel over het al dan niet verwerken van zijn/haar persoonsgegevens door de Nationale ombudsman, bevat het antwoord op het verzoek ten minste (zie art. 15 lid 1 a t/m h AVG):

- de doeleinden van de verwerking;
- de betrokkenen categorieën van persoonsgegevens die worden verwerkt;
- de (categorieën van) ontvangers;
- de bewaartermijnen;
- de mededeling dat de betrokkene het recht heeft te verzoeken dat zijn/haar gegevens worden gerectificeerd of gewist of dat de verwerking wordt beperkt en dat hij/zij het recht heeft om bezwaar te maken;
- de mededeling dat de betrokkene het recht heeft een klacht in te dienen bij de toezichthouder;
- wanneer de gegevens van een andere partij zijn verkregen, alle beschikbare informatie over deze bron.

De standaard tekst voor de reactie is opgenomen in [bijlage 7](#).

3. Inzage persoonsgegevens

In veruit de meeste gevallen gaat het bij de Nationale ombudsman om verzoeken om inzage in het dossier. Als dat het geval is, beoordeelt de behandelend medewerker, in overleg met een AVG vertegenwoordiger, of aan het verzoek tot inzage kan worden voldaan¹. Zo ja, dan moet het dossier opgeschoond worden. De betrokkene heeft slechts recht op inzage voor zover het zijn/haar eigen persoonsgegevens betreft. Persoonlijke aantekeningen, interne correspondentie en het verslag van de Braingain of raadkameroverleg moeten uit het dossier verwijderd worden. Ook moeten de persoonsgegevens van anderen uit het dossier verwijderd worden. Met andere woorden: de betrokkene krijgt alleen inzage in stukken waarin zijn/haar persoonsgegevens voorkomen.

E-mailverkeer met overheidsinstanties en tussen medewerkers kan onderdeel uitmaken van de inzage.

Aanbevolen wordt daarom ook om de correspondentie zakelijk te houden. Zie ook het [beleid omtrent de aanhef van e-mails](#).

¹ Bij twijfel kan worden overlegd met de FG.

Vaak wordt ervoor gekozen om kopieën te maken uit het dossier en deze op te sturen aan verzoeker. Uiteraard is het ook mogelijk om verzoeker uit te nodigen op het bureau om het dossier in te zien. Dit is echter tijdrovender omdat ook in dat geval het dossier van te voren moet worden doorgenomen, eventueel stukken moeten worden verwijderd en stukken moeten worden geanonimiseerd. Inzage wordt slechts verleend in de aanwezigheid van een medewerker, ter voorkoming dat stukken uit het dossier worden verwijderd.

4. Ontvangen kopie persoonsgegevens

Een kopie van persoonsgegevens kan op verzoek worden verstrekt als we hebben geverifieerd dat het de betrokkene zelf is die hierom vraagt en het recht om een kopie te verkrijgen geen afbreuk doet aan de rechten en vrijheden van anderen (art. 15 lid 3 en lid 4 AVG). Het is van belang om persoonsgegevens van anderen te anonimiseren, alvorens de kopieën te verstrekken. Het gaat hierbij dus niet om kopieën van hele dossiers.

5. Rectificatie: correctie / aanvulling persoonsgegevens

Onder rectificatie valt het verbeteren en/of aanvullen van persoonsgegevens. Rectificatie kan worden verzocht als de persoonsgegevens:

- feitelijk onjuist zijn;
- onvolledig zijn of niet ter zake doen voor het doel waarvoor deze zijn verzameld;
- op een andere manier in strijd met de wet worden gebruikt.

Wanneer een verzoek om rectificatie gegrond is, moeten de partijen waarmee de gegevens zijn gedeeld op de hoogte worden gesteld van het verzoek (art. 19 AVG). De rectificatie moet zonder onredelijke vertraging geschieden (art. 16 AVG).

Let op! Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen. Wel mag diegene van de organisatie verwachten dat deze in ieder geval zijn schriftelijke mening toevoegt aan het dossier. Dat kan vooral een oplossing bieden bij situaties waarbij het om niet objectief vast te stellen feiten gaat.

6. Recht op verwijdering van gegevens en het recht op vergetelheid

Verwijdering van persoonsgegevens kan worden verzocht als:

- de gegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld;
- de betrokkene zijn/haar eerder gegeven toestemming intrekt en er geen andere grondslag voor verwerking is;
- de betrokkene bezwaar maakt tegen de verwerking van zijn/haar persoonsgegevens (art. 21 AVG);
- de persoonsgegevens onrechtmatig zijn verwerkt;
- de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting.

Persoonsgegevens hoeven (voor zover relevant) niet gewist te worden als de verwerking nodig is voor het nakomen van een wettelijke verplichting of voor het vervullen van een taak van algemeen belang. Wissing hoeft ook niet plaats te vinden als de verwerking nodig is met het oog op archivering (art. 17 lid 3 AVG). Wanneer een verzoek tot gegevenswissing gegrond is, moeten de partijen met wie de gegevens zijn gedeeld op de hoogte worden gesteld van het verzoek om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen (art. 17 lid 2 en art. 19 AVG). De gegevenswissing moet zonder onredelijke vertraging geschieden.

Let op! Zoals hierboven al staat zijn deze rechten niet van toepassing wanneer dit recht archivering met het oog op het algemeen belang onmogelijk dreigt te maken of deze ernstig in het gedrang dreigt te brengen. Dit betekent dat een verzoeker ons niet kan vragen een dossier of stukken daaruit te vernietigen voordat de bewaartermijn is verstreken.

7. Beperking van verwerking persoonsgegevens

Beperking van de verwerking (pauzeren) kan worden verzocht als (art. 18 lid 1 AVG):

- de juistheid van de persoonsgegevens wordt betwist; de beperking geldt dan gedurende de periode die de Nationale ombudsman in staat stelt de juistheid van de persoonsgegevens te controleren;

- de verwerking onrechtmatig is en betrokkene zich in plaats van op het recht op gegevenswissing beroept op het recht op beperking;
- de gegevens niet meer nodig zijn voor de verwerkingsdoeleinden, maar betrokkene deze nodig heeft voor het instellen, uitoefenen of onderhouden van een rechtsvordering;
- de betrokkene bezwaar heeft gemaakt tegen verwerking.

Wanneer om beperking van de verwerking van persoonsgegevens is verzocht, en dit verzoek is gegrond, kan de Nationale ombudsman zelf bepalen hoe die beperking wordt vormgegeven (ow. 67 AVG). Voorbeelden van hoe gegevensverwerkingen kunnen worden beperkt zijn:

- de geselecteerde persoonsgegevens tijdelijk overbrengen naar een ander verwerkingssysteem;
- de geselecteerde gegevens voor gebruikers tijdelijk niet beschikbaar maken; of
- de gepubliceerde gegevens tijdelijk van een website halen.

Als de verwerking is beperkt, mogen de gegevens (voor zover relevant) alleen nog worden verwerkt met de toestemming van de betrokkene, ter bescherming van de rechten van anderen of om gewichtige redenen van algemeen belang voor de Europese Unie of voor een lidstaat (art. 18 lid 2 AVG). Als een verzoek tot beperking van de verwerking gegrond is, moeten de partijen met wie de gegevens zijn gedeeld op de hoogte worden gesteld (art. 19 AVG).

8. Overdracht persoonsgegevens (dataportabiliteit)

De verwachting is dat bij de Nationale ombudsman niet vaak een beroep zal worden gedaan op het recht op overdracht van de persoonsgegevens (art. 20 AVG). Bovendien sluit artikel 20 lid 3 van de AVG het recht op gegevensoverdracht uit wanneer "... de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend." Bij de Nationale ombudsman vallen de verwerkingen van het primaire proces binnen dit kader, zodat aan een dataportabiliteitsverzoek niet voldaan hoeft te worden. Vanzelfsprekend moet de afwijzing van het verzoek worden gemotiveerd.

9. Geautomatiseerde besluitvorming

Geautomatiseerde besluitvorming (art. 22 AVG) komt bij de Nationale ombudsman niet voor. Het is dan ook niet te verwachten dat verzoeken zullen worden ingediend om daaraan niet onderworpen te worden. Mocht dat toch het geval zijn, dan zal de afwijzing van het verzoek gemotiveerd moeten worden.

LET OP !!!

Als een verzoek betrekking heeft op een door betrokkene ingediende klacht, dan zijn de rechten van betrokkene beperkt. De verwerking van persoonsgegevens tijdens de klachtbehandeling berust namelijk niet op toestemming, dus die kan betrokkene ook niet intrekken.

5 Registratie en archivering van verzoeken

Het verzoek, het antwoord op het verzoek en alle tussenliggende (schriftelijke) correspondentie worden opgenomen in het betrokken Verseen dossier. Is er geen dossier, dan wordt een dossier aangemaakt.

Let op! Gaat het om een verzoekdossier dat al is afgehandeld: de afhandelingsdatum van het betrokken dossier verandert niet, die blijft staan op de eerder gekozen afhandelingsdatum. Door in het veld 'Activiteit' op het tabblad 'Behandeling' te kiezen voor 'nazorg' wordt het afgehandelde dossier zichtbaar in je digitale kast 'afgehandeld'.

6 Afhandeling van bezwaar en klachten

De AVG voorziet in nog twee andere dan de in [bijlage 1](#) genoemde verzoeken. Het gaat om het recht om tegen de gegevensverwerking bezwaar te maken en om het recht om een klacht in te dienen bij de toezichthouder over de wijze waarop persoonsgegevens zijn verwerkt.

6.1 Bezwaar

Een betrokkene kan op grond van art. 21 AVG bezwaar maken tegen de verwerking van zijn gegevens. In drie situaties is de uitoefening van het recht op bezwaar mogelijk:

- bezwaar vanwege persoonlijke omstandigheden tegen verwerkingen die gebaseerd zijn op de grondslagen:
 - a. noodzakelijk voor de uitoefening van een taak van algemeen belang of openbaar gezag; of
 - b. het gerechtvaardigd belang van de verwerkingsverantwoordelijke;
- bezwaar tegen verwerkingen met het oog op direct marketing;
- bezwaar tegen verwerkingen voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden op grond van specifiek met de situatie van betrokkene verband houdende redenen.

Maakt een betrokkene bezwaar vanwege persoonlijke omstandigheden, dan moeten wij de verwerking staken, tenzij er dwingende, gerechtvaardigde gronden zijn waardoor het verwerkingsbelang groter is dan het belang van de betrokkene om de verwerking te laten staken (ow. 69 en art. 21 lid 1 AVG).

Bezwaren worden behandeld door de behandelend medewerker van het betrokken dossier in overleg met een AVG vertegenwoordiger².

6.2 Klacht

Een betrokkene heeft op grond van art. 77 AVG het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens indien hij/zij van mening is dat de verwerking van hem/haar betreffende persoonsgegevens inbreuk maakt op de AVG.

Op onze website wijzen wij mensen op de mogelijkheid hierover eerst contact met ons op te nemen.

'...Heeft u een klacht over het gebruik van uw persoonsgegevens door de Nationale ombudsman, dan kunt u daarover contact met ons opnemen. Ook kunt u daarover een klacht bij ons indienen. Komt u er samen met ons niet uit, dan kunt u uw klacht indienen bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op het gebruik van persoonsgegevens....'

Verder kan betrokkene een klacht indienen bij de AP wanneer wij geen gevolg hebben gegeven aan een verzoek (art. 12 lid 4 AVG). Daarnaast is denkbaar dat een klacht wordt ingediend over de wijze waarop een verzoek is afgehandeld.

7 Ondertekening brieven

Uitgangspunt is dat klachtbehandelaars en onderzoekers zelf de stukken tekenen in de verzoekdossiers die zij in behandeling hebben, tenzij de bevoegdheid niet door de ambtsdaggers is gemandateerd (zie mandaatbesluit van 30 april 2015, Staatscourant 2015 nr. 11998). De behandeling van AVG verzoeken is niet uitgezonderd van het mandaat. Klachtbehandelaars en onderzoekers mogen brieven hierover dus zelf tekenen. Ook hier geldt dat de klachtbehandelaar of onderzoeker zichzelf wel steeds de vraag stelt of bepaalde zaken behalve met de AVG vertegenwoordiger en/of FG besproken moeten worden met bijvoorbeeld de teamleider of een ambtsdrager.

AVG verzoeken t.a.v. andere dan verzoekdossiers zullen zich niet snel voordoen. Krijg je hier toch mee te maken, neem dan contact op met het Bestuursbureau.

² Bij twijfel kan worden overlegd met de FG.

Bijlage 1 Mogelijke AVG-verzoeken

Type verzoek	Artikel AVG
1. Intrekken toestemming verwerking persoonsgegevens	Art. 7 lid 3 AVG
2. Informatie over verwerking persoonsgegevens	Art. 15 lid 1 AVG
3. Inzage persoonsgegevens	Art. 15 lid 1 AVG
4. Ontvangen kopie persoonsgegevens	Art. 15 lid 3 AVG
5. Rectificatie: correctie / aanvulling persoonsgegevens	Art. 16 AVG
6. Gegevenswissing: verwijdering van persoonsgegevens	Art. 17 AVG
7. Beperking van verwerking persoonsgegevens	Art. 18 AVG
8. Overdracht persoonsgegevens (dataportabiliteit)	Art. 20 AVG
9. Geautomatiseerde besluitvorming	Art. 22 AVG

Bijlage 2 Ontvangstbevestiging

De Nationale ombudsman heeft op [datum ontvangst] uw verzoek van [datum verzoek] ontvangen.

Uw verzoek wordt in behandeling genomen en u verneemt zo snel mogelijk, uiterlijk binnen vier weken, nader bericht.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Bijlage 3 Checklist ter voorbereiding op de beantwoording van het verzoek

Vraag	Toelichting	Artikel AVG
1. Kan de betrokkene worden geïdentificeerd?	<u>Zo ja</u>: ga naar vraag 2. <u>Zo nee</u>: vraag om aanvullende informatie die nodig is ter bevestiging van de identiteit. Blijft identificatie uit? Dan luidt het antwoord op het verzoek dat er geen gevolg aan wordt gegeven.	Art. 12 lid 6 AVG
2. Is recentelijk een (inzage)verzoek gedaan?	<u>Zo ja</u>: een verzoek kan worden geweigerd als het kennelijk ongegrond of buitensporig is (vanwege het repetitieve karakter). In dat geval luidt het antwoord op het verzoek dat er geen gevolg aan wordt gegeven. <u>Zo nee</u>: ga naar vraag 3.	Art. 12 lid 5 AVG
3. Is het verzoek gespecificeerd?	<u>Zo ja</u>: ga naar vraag 4. <u>Zo nee</u>: vraag om specificatie, met name wanneer een grote hoeveelheid gegevens wordt verwerkt van de betrokkene. Blijft specificatie uit? Dan kan het verzoek worden geweigerd, omdat het kennelijk ongegrond of buitensporig is (vanwege het repetitieve karakter). In dat geval luidt het antwoord op het verzoek dat er geen gevolg aan wordt gegeven.	Ow. 63 AVG Art. 12 lid 5 AVG
4. Is sprake van persoonsgegevens?	<u>Zo ja</u>: ga naar vraag 5. <u>Zo nee</u>: het antwoord luidt dat van de betrokkene geen persoonsgegevens worden verwerkt.	
5. Is de AVG van toepassing op de persoonsgegevens?	<u>Zo ja</u>: ga naar vraag 6. <u>Zo nee</u>: het antwoord luidt dat geen gevolg wordt gegeven aan het verzoek. AVG is van toepassing op (gedeeltelijk) geautomatiseerde verwerking en op verwerking die in bestand is opgenomen. Een bestand is elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.	Ow. 15 AVG
6. Is de betrokkene al op de hoogte van de persoonsgegevens?	<u>Zo ja</u>: persoonsgegevens waarover de betrokkene al beschikt en waarvan hij zich al een oordeel heeft kunnen vormen, hoeven niet te worden verstrekt. Denk aan: - stukken van of aan (de gemachtigde van) betrokkene; - persoonsgegevens in concept voor zover gelijk aan de definitieve versie; of - een reactie op een vorig verzoek. Het antwoord luidt dan dat geen gevolg wordt gegeven aan het verzoek. <u>Zo nee</u>: ga naar vraag 7. N.B. Inzagerecht omvat meer dan de plicht tot kennisgeving van persoonsgegevens, bv kennisgeving van doelen en bewaartermijn.	
7. Is sprake van een weigeringsgrond?	<u>Zo ja</u>: het antwoord luidt dat geen gevolg wordt gegeven aan het verzoek dan wel – als er op een deel van de persoonsgegevens geen weigeringsgrond van toepassing is –	Art. 23 AVG

dat het verzoek wordt beperkt.
Zo nee: het verzoek wordt ingewilligd.

N.B. Onder de rechten en vrijheden van "anderen" (art. 23 sub I AVG) moet ook de Nationale ombudsman worden begrepen. Vertrouwelijkheid van informatie kan ook onder het beschermingsbereik van art. 23 sub I AVG vallen.

Bijlage 4 Antwoord: geen persoonsgegevens

Naar aanleiding van uw verzoek van [datum verzoek] bericht ik u als volgt.

U bent bij de Nationale ombudsman niet bekend. Er worden geen persoonsgegevens van u door de Nationale ombudsman verwerkt.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Bijlage 5 Redenen om geen gevolg te geven / verzoek te beperken

Redenen om geen gevolg te geven aan een verzoek

- | | |
|--|---|
| 1. De AVG is van toepassing omdat: <ul style="list-style-type: none">- de gegevens worden verwerkt met het oog op voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten.- de gegevens worden verwerkt met het oog op de tenuitvoerlegging van strafrechtelijke sancties;- de gegevens worden verwerkt in het kader van de bescherming tegen en voorkoming van gevaren openbare veiligheid/nationale veiligheid.- de rechten en vrijheden van anderen dienen te worden beschermd. | Art. 2 lid 2 sub d AVG |
| <hr/> | |
| 2. Nadat aanvullende gegevens zijn gevraagd, is identificatie van de betrokkene nog steeds niet mogelijk | Art. 11 lid 2 juncto
Art. 12 lid 2 AVG |
| <hr/> | |
| 3. Het verzoek is buitensporig (repetitief) | Art. 12 lid 5 AVG |
-

Redenen om het verzoek te beperken

- | | |
|--|-------------|
| Een wettelijke grondslag maakt beperking van het verzoek mogelijk, mits die beperking de grondrechten en fundamentele vrijheden onverlet laat en een noodzakelijke en evenredige maatregel is ter waarborging van: <ul style="list-style-type: none">a. De nationale veiligheid;b. Landsverdediging;c. Openbare veiligheid;d. Voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, incl. bescherming en voorkoming van gevaren voor openbare veiligheid;e. Doelstellingen van de EU of van een lidstaat (economisch/financieel, monetair, budgettair, fiscaal, volksgezondheid en sociale zekerheid);f. Bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;g. De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van beroepsregels voor gereguleerde beroepen;h. Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van openbaar gezag in de bovengenoemde gevallen (m.u.v. punt f.);i. Bescherming van betrokkene of rechten en vrijheden van anderen;j. Inning van civielrechtelijke vorderingen | Art. 23 AVG |
|--|-------------|
-

Bijlage 6 Antwoord: geen gevolg geven / verzoek beperken

Geen gevolg geven aan verzoek

Naar aanleiding van uw verzoek van [datum verzoek] bericht ik u als volgt.

Uw verzoek wordt niet in behandeling genomen, omdat [reden afwijzing].

Als u niet tevreden bent met de wijze waarop uw verzoek is afgehandeld, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Verzoek beperken

Naar aanleiding van uw verzoek van [datum verzoek] bericht ik u als volgt.

Er is een wettelijke grondslag die maakt dat uw verzoek wordt beperkt. Beperking van uw verzoek is een noodzakelijke en evenredige maatregel ter waarborging van [reden genoemd in art. 23 sub a t/m j AVG].

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Bijlage 7 Antwoord: Informatie over verwerking persoonsgegevens

U heeft op [datum verzoek] een verzoek gedaan om inzage van de persoonsgegevens die de Nationale ombudsman van u verwerkt.

Uw gegevens worden verwerkt in de volgende verwerkingen:

- [naam verwerking]
- [naam verwerking]
- ...

De bijlage bevat per verwerking een overzicht van de verwerkingsverantwoordelijke, de verwerkingsdoeleinden, de categorieën persoonsgegevens die worden verwerkt, van wie de Nationale ombudsman de gegevens heeft ontvangen, de (categorieën van) ontvangers aan wie de gegevens zijn of kunnen worden verstrekt en informatie over de bewaartermijn van uw gegevens.

U heeft het recht de verwerkingsverantwoordelijke te verzoeken om het rectificeren, wissen of beperken van de verwerking van de persoonsgegevens. Ook kunt u bezwaar maken tegen de verwerking van uw persoonsgegevens.

Als u niet tevreden bent met de wijze waarop uw verzoek is afgehandeld, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Onderwerp	toelichting	Categorie	Wie	status
1 Beveiliging SRVODB server	De verseon DB draait op de SRVODB. Zowel de database als de fileserver zijn niet voorzien van encryptie. Onderzoeken welke maatregelen er extra genomen kunnen worden om de beveiliging van de database en server zo sterk mogelijk te maken.	Informatiebeveiliging	██████	open
2 Proces datalek melding stroomlijnen	Op dit moment wordt een datalek in Topdesk en in BureauDok geregistreerd. De toekomst van Topdesk is niet zeker. Wellicht kan de datalekregistratie compleet worden overgeheveld naar BureauDok. Tevens kijken naar verantwoordelijkheid en afhandeling van melding. Dit ligt nu bij de FG, maar is wellicht beter op z'n plek bij de Sector- en afdelingshoofden.	AVG	██████ BB	open
3 Datalek melding	Op NoHow het melden van een datalek laagdrempeliger maken. Bijvoorbeeld een apart item in een menu 'meld een datalek'. Bezoekers van de website en het gebouw van de No worden (via een disclaimer en privacy statement) geïnformeerd dat op een veilige en rechtmatige wijze met hun persoonsgegevens wordt omgegaan en worden gewezen op de rechten die ze hebben conform de AVG.	AVG	██████ / C&M	open
4 Privacy Statement Website		AVG	BB	afgehandeld
5 Bewaartermijnen dossiers	Minimale bewaartermijn voor zaken is nu 5 jaar. Dit geldt ook voor buitenwettelijke dossiers. Deze termijnen moeten opnieuw onderzocht worden om te bepalen of deze periodes verkort kunnen worden. Dit zal in 2019 worden opgepakt.	AVG	BB	open
6 Handtekening op ontvangstbevestiging	OVB's zijn voorzien van handtekeningen. De vraag is of dit wenselijk is in het kader van vervalsing/fraude.	Informatiebeveiliging	BB	open
7 BSN nummer Verseon	In Verseon is een apart veld voor BSN opgenomen bij de NAW gegevens. De No gebruikt het BSN optioneel alleen voor zaken over de belastingdienst en UWV. BSN als apart attribuut lijkt niet nodig en dient uit Verseon verwijderd te worden. Protocol moet verder worden aangescherpt i.v.m. foto's en dus gebruik van persoonsgegevens. Na aanpassing ook uitdragen binnen de organisatie.	AVG	FD	open
8 protocol social media	Er staan een aantal camera's opgesteld in en rond de panden waardoor bezoekers vastgelegd kunnen worden. Er moet bij deze camera's een vermelding komen dat dit gebeurt.	AVG	C&M	afgehandeld
9 Informeren over cameratoezicht	Hoe lang wordt een mailbox bewaard? Enterprise Vault? Proces voor inzage in mailbox of journal (bijv. met toestemming van Directeur).	AVG	FD	afgehandeld
10 procedure voor vernietiging en inzage mailboxen medewerkers	Hoe om te gaan met VIP lijsten. Alleen Verseon zou de bron voor VIP lijsten moeten zijn. VIP lijst is nu ook op NoHow zichtbaar. Hoe lang blijft iemand op een VIP lijst?	AVG / informatiebeveiliging	BB	open
11 VIP lijsten	Bij uitdiensttreding wordt de mailbox vernietigd. Enterprise Vault wordt echter niet opgeruimd. Hier moet wat voor worden ingericht.	AVG	BB	open
12 Enterprise vault		AVG / informatiebeveiliging	ICT	open
13 Verwerkingsovereenkomst Circle	Circle geeft aan zichzelf niet als verwerker te zien, maar wel indien gewenst een overeenkomst te willen ondertekenen.	AVG	BB	open
14 Register voor integriteitsschendingen	Moet nog ingericht worden.		BB	open
15 disclaimer onder emails	disclaimer onder emails opnemen dat indien een bericht niet bestemd is voor de lezer, deze weggegooid moet worden	AVG	BB	open
16 Toestemming voordat zaaken de KEN in worden gestuurd.	Zie notitie ██████ J AVG - Archiefwet. Hoe dit in te regelen?	AVG	BB	open
17 autorisatie structuur in Verseon	Alle onderzoekers kunnen nu ook alle klachten inzien. Vraag is of dat niet te ruim is. ██████ J onderzoekt wat de mogelijkheden zijn voor meer fine-grained autorisatie.	AVG	FD	open
18 Google Analytics vervangen door Piwik op site		AVG	C&M	open

Privacy Impact Assessment (PIA)

Hierin staan de actuele risico's met betrekking tot de bescherming van persoonsgegevens beschreven.

Juni 2018

Inhoud

1	Algemeen.....	4
1.1	Over deze Privacy Impact Assessment.....	4
1.1.1	Doelstelling	4
1.1.2	Scope	4
1.1.3	Proces	4
1.1.4	Informatiebronnen en betrokkenen.....	4
2	Verwerking van persoonsgegevens binnen de Nationale ombudsman.....	5
2.1	Hoofdprocessen met verwerking van persoonsgegevens.....	5
2.1.1	Medewerkers.....	5
2.1.2	Overige.....	5
2.2	Informatiebeveiliging	5
3	Persoonsgegevens: primair proces.....	6
3.1	Soorten persoonsgegevens en informatiestromen.....	6
3.1.1	Gegevensverzamelingen	6
3.1.2	Verwerkingen met hoog risico	6
3.2	Verzamelen en afleiden van persoonsgegevens.....	6
3.3	Gebruik van de persoonsgegevens	7
3.4	Beschikbaar maken en delen van persoonsgegevens	7
3.5	Bewaren, vernietigen en archiveren van persoonsgegevens.....	7
3.5.1	Bewaartermijnen.....	7
3.5.2	Nationaal archief, archiefwet	7
4	Persoonsgegevens: medewerkers	9
4.1	Soorten persoonsgegevens en verwerkingen	9
4.1.1	Gegevensverzamelingen	9
4.1.2	Verwerkingen	11
4.2	Verzamelen en afleiden van persoonsgegevens.....	11
4.3	Gebruik van de persoonsgegevens	11
4.4	Beschikbaar maken en delen van persoonsgegevens	13

4.5	Bewaren, vernietigen en archiveren van persoonsgegevens	13
4.5.1	Bewaartermijnen	13
5	Persoonsgegevens: overige	14
5.1	Soorten persoonsgegevens en informatiestromen	14
5.1.1	Bezoekersregistratie	14
5.1.2	Publicaties	14
5.1.3	Website	14
5.1.4	Bewaartermijnen	15
6	Privacy assessment (Risico-inventarisatie)	16
6.1	Primair proces	16
6.2	Medewerkers	18
6.3	Overige	20
7	Aanbevelingen om impact op privacy te verkleinen	21
7.1	Primair proces	21
7.2	Medewerkers	23
7.3	Overige	24
8	Bijlage: overzicht verwerkingen	25
8.1	Primair proces	25
8.2	Bedrijfsvoering (medewerkers en overige)	25

1 Algemeen

1.1 Over deze Privacy Impact Assessment

1.1.1 Doelstelling

Deze Privacy Impact Assessment (PIA) is een risicoanalyse gericht op de wijze waarop de Nationale ombudsman (No) persoonsgegevens verwerkt. Deze PIA bevat een momentopname van de verwerkingen. Op basis hiervan zijn de risico's voor No en de persoonlijke levenssfeer van betrokkenen in kaart gebracht. Vervolgens zijn deze risico's beoordeeld en worden aanbevelingen gedaan voor het mitigeren van de relevante risico's.

1.1.2 Scope

De scope van deze PIA is de verwerking van persoonsgegevens waarvoor - op basis van een eerste beoordeling - waarbij het minimaliseren van risico's wordt nagestreefd. De PIA heeft betrekking op de gehele organisatie en alle fasen van de informatie levenscyclus, voor de relevante gegevensverwerkingen.

1.1.3 Proces

Voor het bepalen van de privacy risico's is de volgende aanpak gehanteerd:

1. De hoofdprocessen en het doel kort beschrijven (hoofdstuk 2)
2. In kaart brengen relevante persoonsgegevens en maatregelen (hoofdstuk 3)
3. PIA-workshops waarin privacy risico's zijn geïdentificeerd (hoofdstuk 4)
4. Aanbevelingen formuleren voor verkleinen van de impact op privacy (hoofdstuk 5)

De resultaten hiervan zijn opgenomen in deze PIA.

1.1.4 Informatiebronnen en betrokkenen

De PIA is gebaseerd op de volgende informatie:

- Register van verwerkingen van persoonsgegevens van de No
- Interviews met medewerkers met relevante proceskennis
- Informatiebeveiligingsbeleid
- Statements op de website van de No

Bij het opstellen van deze PIA is een brede vertegenwoordiging van No-disciplines betrokken, waaronder de volgende rollen:

- Functionaris gegevensbescherming
- CFO / Informatiebeveiliging
- Hoofd bestuursbureau
- Adviseur HR
- (Senior) onderzoeker
- Functioneel Applicatie beheerder
- Extern adviseur gegevensbescherming

2 Verwerking van persoonsgegevens binnen de Nationale ombudsman

2.1 Hoofdprocessen met verwerking van persoonsgegevens

De hoofdprocessen waarbij persoonsgegevens worden verwerkt door de No zijn te groeperen rond drie soorten persoonsgegevens:

1. Primair proces
2. Medewerkers
3. Overige

Bovenstaande activiteiten zijn onderdeel van de standaard werkwijze van de organisatie.

2.1.1 Medewerkers

Gegevens van medewerkers worden verwerkt voor gebruikelijke activiteiten zoals persoonlijke ontwikkeling, loopbaanbegeleiding, het voeren van een personeels- en salarisadministratie, en werving- en selectie.

2.1.2 Overige

De No verzamelt en onderhoud een set gegevens van haar relaties, ten behoeve van het onderhouden van contacten. Het gaat hierbij vooral om de zakelijke contactgegevens van personen die werkzaam zijn bij andere organisaties.

Ook wordt het klikgedrag op de website bijgehouden ten behoeve van het verbeteren van de gebruikerservaring.

2.2 Informatiebeveiliging

De No beschikt over een actueel beleid voor informatiebeveiliging en een set passende maatregelen waarmee informatie in de organisatie wordt beveiligd.

De persoonsgegevens die de No verwerkt, worden hiermee adequaat beveiligd.

3 Persoonsgegevens: primair proces

In dit hoofdstuk wordt beschreven welke persoonsgegevens door de No worden verwerkt in het primair proces, op welke wijze dit plaatsvindt en welke gerichte maatregelen zijn getroffen of voorzien.

3.1 Soorten persoonsgegevens en informatiestromen

De volgende gegevenssoorten worden door de No verwerkt in het primair proces:

- Klachten van burgers
- Klachten van burgers mbt kinderen
- Klachten van veteranen

3.1.1 Gegevensverzamelingen

De persoonsgegevens voor klachtbehandeling bestaan uit NAW van de klager en overige betrokken personen en contactgegevens van personen bij instanties. Afhankelijk van het soort klacht kunnen ook financiële gegevens, beoordelingen, in het dossier zitten. Dit zijn reguliere gegevens.

Ook kunnen medische of strafrechtelijke gegevens en het BSN onderdeel zijn van het dossier, wat bijzondere persoonsgegevens zijn onder de AVG.

Alle gegevens uit deze categorie worden verwerkt op basis van het uitvoeren van een wettelijke taak.

Het doel, de grondslag en de bewaartermijnen van de verschillende persoonsgegevens zijn vastgelegd in het register van gegevensverwerkingen van de No. Dit register is in opbouw en derhalve nog niet volledig.

3.1.2 Verwerkingen met hoog risico

De verwerkingen die mogelijk kunnen leiden tot een hoog risico zijn:

- M3313 - Klachtbehandeling Veteranenombudsman
- M1846 - Klachtbehandeling, en onderzoek uit eigen beweging, door de Nationale ombudsman
- ~~M2881 - Verwerken van AIVD documenten in Verseon~~ (*)
- M2879 - Registreren van NAW gegevens in Verseon (**)
- M1902 - Klachtbehandeling kinderombudsman
- M1898 - Het online stellen van vragen aan de Kinderombudsman

(*) Deze verwerking is onlangs komen te vervallen

(**) Dit is een deelproces van de klachtbehandelingsprocessen en wordt daarom niet als apart proces behandeld

3.2 Verzamelen en afleiden van persoonsgegevens

De gegevens voor klachtbehandeling worden aangeleverd door de betrokkenen.

In een deel van de gevallen worden aanvullende gegevens verkregen van de overheidsinstelling waar de klacht betrekking op heeft.

3.3 Gebruik van de persoonsgegevens

De persoonsgegevens van medewerkers worden gebruikt in de processen voor klachtbehandeling.

De gegevens van betrokkenen worden naast behandeling van individuele klachten, gebruikt voor het signaleren van trends door de No en het communiceren van (geanonimiseerde) voorbeeldzaken in het jaarverslag van de No.

Er wordt niet gebruik gemaakt van geautomatiseerde besluitvorming.

3.4 Beschikbaar maken en delen van persoonsgegevens

Iedere klachtbehandelaar uit het team waarin de klacht wordt behandeld, maar ook medewerkers in ondersteunende rollen, hebben toegang tot de persoonsgegevens van betrokkenen.

Betrokkenen kunnen via een informatieverzoek inzage krijgen in de gegevens die de No over hen verwerkt. Over deze mogelijkheid worden betrokkenen geïnformeerd via het privacy statement op de website.

Persoonsgegevens van klagers en overige betrokkenen bij een klacht worden in voorkomende gevallen gedeeld met de betrokken instellingen, voor het opvragen van relevante informatie of bij het bemiddelen in de klachtbehandeling.

Er zijn geen geautomatiseerde leveringen van persoonsgegevens aan externe partijen.

3.5 Bewaren, vernietigen en archiveren van persoonsgegevens

Alle gegevens over klachten worden bewaard in het DMS Verseon. Toegang tot de dossiers is beperkt tot No-medewerkers. Er is geen verdere verbijzondering van de toegangsrechten per dossier, iedere medewerker kan alle dossiers inzien. De enige uitzondering hierop is de toegang tot dossiers die als vertrouwelijk zijn aangemerkt, dit zijn met name klachten die betrekking hebben op de No.

De gegevens worden door de No in de eigen infrastructuur in Den Haag opgeslagen. Het functioneel beheer op Verseon wordt door de No zelf verzorgd, het technisch beheer is uitbesteed aan Circle.

3.5.1 Bewaartermijnen

De bewaartermijnen van de verschillende persoonsgegevens zijn vastgelegd in het register van gegevensverwerkingen van de No en in de selectielijst voor de No.

3.5.2 Nationaal archief, archiefwet

Op basis van een verplichting vanuit de Archiefwet wordt een selectie van relevante dossierstukken overgedragen aan het Nationaal archief. Deze stukken worden binnen de No na overdracht vernietigd. Overige stukken worden eerder, na een vastgestelde termijn,

vernietigd. De keuze om te bewaren en over te dragen naar het Nationaal Archief of om te vernietigen, is vastgelegd in de selectielijst voor de Nationale ombudsman.

4 Persoonsgegevens: medewerkers

In dit hoofdstuk wordt beschreven welke persoonsgegevens door de No worden verwerkt over medewerkers, op welke wijze dit plaatsvindt en welke gerichte maatregelen zijn getroffen of voorzien.

4.1 Soorten persoonsgegevens en verwerkingen

De volgende gegevenssoorten worden door de No verwerkt:

- Personeelsgegevens
- Opleidingen
- Salarisgegevens
- Geheimhoudingsverklaring
- Bruikleenovereenkomsten
- Ziektemeldingen
- ARBO dossiers en re-integratie-informatie
- Sollicitanten
- ICT- en netwerkadministratie (gebruikersaccounts)

4.1.1 Gegevensverzamelingen

De gegevens bestaan uit gewone gegevens die voor een personeelsdossier vereist zijn, waaronder NAW, burgerlijke staat, salaris, beoordelingen en dergelijke. In de personeelsadministratie wordt het Rijks Identificatie Nummer (RIN) bijgehouden, in de plaats van het BSN. De geheimhoudingsverklaring en bruikleenovereenkomsten bevatten uitsluitend de gegevens die nodig zijn om de overeenkomst medewerkers met de medewerker te kunnen sluiten (NAW).

De ziektemeldingen bevatten geen medische gegevens, deze blijven bij de ARBO-dienst. De ARBO-dienst houdt voor begeleiding een inhoudelijk dossier bij, waarvoor de No de verwerkingsverantwoordelijke is. De afdeling HR slaat gegevens op die benodigd zijn voor het faciliteren van re-integratie van medewerkers. Dit zijn bijzondere persoonsgegevens. Op de G-schijf worden onder andere Functie-Mogelijkheden Lijsten (FML) opgeslagen. De toegang is beperkt tot HR-medewerkers.

In P-Direkt / IKAP wordt lidmaatschap van de vakbond geregistreerd ivm tegemoetkoming in de kosten door de No. Dit is een bijzonder persoonsgegeven. Het risico is echter laag, omdat alleen P-Direkt hier toegang toe heeft.

In het kader van BHV kunnen medewerkers op vrijwillige basis medische informatie aanleveren. Dit zijn bijzondere persoonsgegevens. Medewerkers moeten zelf het initiatief nemen voor het aanleveren van deze informatie. Deze informatie is opgeslagen in BureauDok met status vertrouwelijk en is alleen toegankelijk voor EHBO'ers en het hoofd BHV.

De No huurt voor specifieke opdrachten ZZP'ers in. Van deze ZZP'ers worden alleen gegevens verwerkt die nodig zijn voor het contracteren en uitvoeren van een opdracht. Dit zijn de zakelijke adresgegevens, tarief en opdrachtbeschrijving. In bepaalde gevallen moet van ZZP'ers en derden ook het identiteitsbewijs met BSN worden aangeleverd opgave

aangifte richting Belastingdienst. De verwerking vindt plaats op basis van een wettelijke verplichting en gebeurt door de manager verantwoordelijk voor inkoop.

Van sollicitanten worden contactgegevens en CV's bewaard.

Het register voor integriteitsschendingen is nog niet ingericht.

4.1.2 Verwerkingen

De processen met een hoog risico zijn volgens het register van verwerkingen:

- M1859 - Personeelsgegevens P-direkt
- M1882 - Volgen en beperken ziekteverzuim medewerkers
- M1912 - Medewerkerstevredenheidsonderzoeken
- M1880 - Uitvoeren bovenwettelijke regelingen
- M1863 - Gebruikmaken van openbaarvervoer kaarten
- M1893 - Het houden van cameratoezicht
- M2882 - Onderhouden relaties in WieNo
- M2387 - Google Analytics
- M1877 - Uitvoeren werving en selectietrajecten personeel met dienstverband en externe inhuur
- M3305 - Vastleggen medische achtergrond No medewerkers
- M3220 - Aanvragen, beheren en onderhouden registratienummer medewerker (RIN)
- M1862 - Behandelen interne klachten
- M1871 - Inventariseren integriteitsschendingen
- M2900 - Nieuwsbrieven

Alle gegevens uit deze categorie worden verwerkt op basis van een wettelijke verplichting of uitvoering van de overeenkomst met de medewerker. Dit kunnen eenzijdige besluiten zijn. Het doel, de grondslag en de bewaartermijnen van de verschillende persoonsgegevens zijn vastgelegd in het register van gegevensverwerkingen van de No. Dit register is in opbouw en derhalve nog niet volledig.

4.2 Verzamelen en afleiden van persoonsgegevens

De gegevens uit deze categorie worden rechtstreeks verkregen van de betrokkene. Bij indiensttreding worden de gegevens door de medewerker verstrekt.

De gegevens van medewerkers worden niet voor andere doelen gebruikt. Het is niet mogelijk voor betrokkenen om zich tegen de verwerking te verzetten omdat deze op basis van een wettelijke verplichting plaatsvinden.

4.3 Gebruik van de persoonsgegevens

De persoonsgegevens van medewerkers worden gebruikt voor gangbare processen zoals salarisbetaling en beoordelingen. De gegevens worden niet voor andere doeleinden (her)gebruikt.

Medewerkers kunnen deelnemen aan Shuttle voor OV-dienstreizen. Alleen zakelijk gebruik is toegestaan. Periodiek wordt de reis-historie door HR gecontroleerd, om misbruik te voorkomen.

Wijzigingen worden door de medewerker aangegeven in P-direkt, of rechtstreeks gemeld aan personeelszaken, die deze wijzigingen verwerkt in de administratie(s). Medewerkers kunnen zelf in P-Direkt hun dossier inzien.

Er wordt niet gebruik gemaakt van geautomatiseerde besluitvorming.

4.4 Beschikbaar maken en delen van persoonsgegevens

Uitsluitend de HR-medewerkers en control en de directe leidinggevende hebben toegang tot persoonsgegevens van medewerkers in P-Direkt. De rechten op de netwerkschijf worden door ICT toegekend, de rechten in P-direct worden door de HR-medewerkers beheerd.

Medewerkers kunnen hun salarisstroken online bekijken, automatisch toegestuurd krijgen en downloaden.

CV's van sollicitanten blijven bij HR en worden uitsluitend gedeeld met de relevante lijnmanager die de sollicitatie zal afhandelen. De CV's worden per interne e-mail gedeeld.

Er zijn geen geautomatiseerde leveringen van persoonsgegevens aan externe partijen.

4.5 Bewaren, vernietigen en archiveren van persoonsgegevens

De personeelsdossiers worden op een afgeschermd deel van P-Direkt bewaard en er zijn nog oude dossiers op papier aanwezig die al vernietigd hadden moeten zijn. De toegang tot de papierendossiers ligt alleen bij de HR-medewerkers.. De salarisadministratie is ondergebracht in een webgebaseerd systeem van P-direct. Voor pensioenen wordt gebruik gemaakt van de webgebaseerde oplossing van ABP.

ARBO-dossiers zijn in beheer bij de arbodienst. Toegang tot de niet-medische gegevens is alleen mogelijk door HR-medewerkers. Hierbij wordt gebruik gemaakt van SMS-authenticatie. De gegevens worden op het grondgebied van de Europese Unie opgeslagen. Met alle betrokken partijen is inmiddels een verwerkersovereenkomst gesloten.

De gegevens ten behoeve van re-integratie van medewerkers worden opgeslagen op de G-schijf en zijn alleen toegankelijk door HR-medewerkers.

De gegevens van ZZP'ers worden opgeslagen in Bureaudok (Verseon) en zijn alleen toegankelijk voor HR en control. Daarnaast zijn factuur-gegevens beschikbaar in de financiële administratie.

De CV's van sollicitanten worden op dit moment veelal bewaard op de netwerkschijf en blijven achter in e-mailboxen van medewerkers. Deze worden niet periodiek opgeschoond.

4.5.1 Bewaartermijnen

De bewaartermijnen van de verschillende persoonsgegevens zijn vastgelegd in het register van gegevensverwerkingen van de No en in de selectielijst voor de No.

5 Persoonsgegevens: overige

In dit hoofdstuk wordt beschreven welke overige persoonsgegevens door de No worden verwerkt, op welke wijze dit plaatsvindt en welke maatregelen zijn getroffen of voorzien.

5.1 Soorten persoonsgegevens en informatiestromen

De volgende gegevenssoorten worden door de No verwerkt:

- Bezoekersregistratie
- Publicaties
- Klikgedrag (Google Analytics)

5.1.1 Bezoekersregistratie

Van bezoekers wordt de naam vastgelegd in Topdesk bij de receptie. Omdat een bezoeker wordt uitgenodigd op een bepaald tijdstip, mag deze er vanuit gaan dat zijn bezoek wordt vastgelegd. Er is geen richtlijn voor vernietiging van deze gegevens,

5.1.2 Publicaties

De No maakt gebruik van fotomateriaal in al haar publicaties. Wanneer er een foto/opname van iemand wordt gemaakt - bijvoorbeeld voor een interview, op een bijeenkomst, een evenement, een beurs, etc. - en de betreffende persoon staat herkenbaar afgebeeld en is dus identificeerbaar, dan vraagde de No de geportretteerde altijd om toestemming om deze foto te mogen gebruiken én bewaren. Dit beleid is in juni 2018 opgesteld en aan medewerkers gecommuniceerd.

5.1.3 Website

Op de website wordt Google Analytics gebruikt voor het bijhouden van klikgedrag van bezoekers. Op de website van de No staat een cookie statement en privacyverklaring. Het is voor bezoekers echter niet duidelijk welke informatie exact wordt verzameld, waar deze is opgeslagen en met wie de data (door Google) wordt gedeeld.

Er worden door de website van No geen niet-functionele cookies geplaatst van Twitter, Facebook en dergelijke. Gebruikers kunnen op een icoon voor Twitter, Facebook of LinkedIn klikken, waarna ze naar de website van deze partners worden doorgestuurd. Gebruikers worden echter niet geïnformeerd over het risico van tracking door deze media, maar wel over het feit dat deze partijen cookies kunnen plaatsen.

De grondslag die voor bovengenoemde bewerkingen wordt gehanteerd is 'gerechtvaardigd belang'. No heeft hierbij het risico voor de betrokkene afgewogen tegen het belang van de organisatie. Volgens de Telecomwet is echter expliciete toestemming vereist voordat niet-functionele cookies mogen worden geplaatst.

Door middel van de privacyverklaring op de website wordt inzicht gegeven in de rechten van de betrokkenen en hoe bezoekers deze bij de No kunnen uitoefenen. Dit privacy statement wordt op dit moment verder gedetailleerd.

5.1.4 Bewaartermijnen

De bewaartermijnen van de verschillende persoonsgegevens zijn vastgelegd in het register van gegevensverwerkingen van de No.

6 Privacy assessment (Risico-inventarisatie)

In dit hoofdstuk staan risico's die van invloed kunnen zijn op de privacy van betrokken personen. Deze risico's zijn geïdentificeerd in de uitgevoerde interviews en workshops.

De risico's met verhoogd risico voor de betrokkene en/of organisatie zijn in rood gemarkeerd. Hiervoor worden in het volgende hoofdstukken maatregelen voorgesteld.

6.1 Primair proces

Risico	Beschrijving	Persoonlijke impact (L/M/H)	Business impact (L/M/H)
P.1	Klachtendossiers in Verseon zijn breed toegankelijk. Hierdoor is de kans op onrechtmatige verwerking (inzien) door iemand die niet rechtstreeks bij de klacht betrokken is aanzienlijk.	H	M
P.2	Er is geen opschoonprocedure voor dossiers in Verseon. Gegevens worden langer bewaard dan noodzakelijk. Risico op onrechtmatig verwerken en grotere impact bij evt. datalekken.	M	M
P.3	Er worden meer persoonsgegevens verzameld en opgeslagen dan strikt noodzakelijk zijn voor de klachtbehandeling. Het gaat hierbij om gegevens die door de klager worden aangeleverd per e-mail of per post die vervolgens wordt gescand. Risico op onrechtmatig verwerken en grotere impact bij evt. datalekken.	M	M
P.4	Gegevens van buitenwettelijke klachten worden te lang bewaard (5 jaar). Risico op onrechtmatig verwerken en grotere impact bij evt. datalekken.	M	M
P.5	NAW-gegevens worden gedeeld tussen de No en KOM, hierdoor kunnen de verkeerde of onjuiste gegevens worden gebruikt voor contact met de klager, waardoor informatie over klachten naar de verkeerde persoon gaat. Daarnaast zijn de NAW-gegevens niet altijd actueel.	H	H
P.6	Het formulier op de website wijzigt waardoor het niet meer mogelijk is om anoniem een klacht in te dienen.	M	L
P.7	Via het formulier op de website worden mogelijk ongewenste/te veel persoonsgegevens verstrekt door de indiener. Deze gegevens worden geregistreerd bij het verzoek.	L	L
P.8	Voor structurele aanpak worden persoonsgegevens uit klachtendossiers gebruikt voor analyse en (geanonimiseerde) voorbeelden. Dit is een ander gebruik dan waarvoor de gegevens zijn verzameld. Hierover is de burger niet geïnformeerd en hiervoor is geen toestemming gevraagd.	M	M

Risico	Beschrijving	Persoonlijke impact (L/M/H)	Business impact (L/M/H)
P.9	Bij mobiel werken is het mogelijk een privé-toestel (smartphone of tablet) te gebruiken voor e-mail van de No. Kans op datalekken bij diefstal en verlies of malware.	M	M
P.10	Het bestand met contactpersonen van de No bevat historische data en is niet altijd actueel. Het gaat hierbij vooral om gegevens van contactpersonen van bestuursorganen.	L	L
P.11	Bij het bemiddelen in of behandelen van klachten wordt veelal contact opgenomen met organisaties. Hierbij wordt informatie gedeeld. Het risico is dat teveel persoonsgegevens worden gedeeld met die organisaties. Risico dat gegevens worden gedeeld zonder de juiste waarborgen en/of na klachtbehandeling achterblijven bij deze organisaties, waarna deze door die organisatie worden (her)gebruikt.	H	L
P.12	De 'VIP'-lijst bevat NAW-gegevens en contactafspraken (incl. beperkingen) van o.a. veelklagers en bijvoorbeeld klagers die schelden. Het lekken van deze lijst zou stigmatiserend werken. De lijst is op dit moment voor iedereen zichtbaar.	H	M
P.13	Via NoHow zijn klachtendossiers te zoeken en in te zien.	H	M
P.14	Informatie over dossiers en klagers wordt <i>intern</i> gedeeld via e-mail. Kans op verkeerd adresseren binnen No (datalek) en te lang bewaren (opslag in e-mail).	M	L
P.15	Informatie over dossiers en klagers wordt <i>extern</i> gedeeld via e-mail. Kans op verkeerd adresseren (datalek) en te lang bewaren door ontvanger (opslag in e-mail).	H	M
	Naw gegevens verzoekers worden los van een dossier opgebouwd en worden niet opgeschoond. Een verzoeker kan gekoppeld worden aan meerdere dossiers. Kans op onnodig koppelen van informatie (bijv. KOM en No)	H	H

6.2 Medewerkers

Risico	Beschrijving	Persoonlijke impact (L/M/H)	Business impact (L/M/H)
M.1	In P-Direkt wordt ten behoeve van diversiteitsbeleid vanuit de overheid, gevraagd naar de afkomst van de ouders van nieuwe medewerkers. Deelname is geheel vrijwillig en anoniem. Of iemand heeft deelgenomen en wat de resultaten zijn is niet zichtbaar voor de No.	L	L
M.2	Medewerkers kunnen deelnemen aan Shuttle voor OV-dienstreizen. Alleen zakelijk gebruik is toegestaan. Periodiek wordt de reis-historie door HR gecontroleerd, om misbruik te voorkomen. Hierdoor zou reisgedrag van medewerkers kunnen worden gevolgd.	L	L
M.3	In P-Direkt / IKAP wordt lidmaatschap van de vakbond geregistreerd ivm tegemoetkoming in de kosten door de No. Dit is een bijzonder persoonsgegeven. Het risico is echter laag, omdat alleen P-Direkt hier toegang toe heeft.	L	L
M.4	De informatie die door HR wordt opgeslagen in het kader van re-integratie van medewerkers worden te lang bewaard en niet opgeschoond. En niet op de juiste plek	M	L
M.5	Medewerkers vragen aan HR soms privé adressen op voor het sturen van een kaartje bij gebeurtenissen (zoals geboorte van kinderen of overlijden). Hiervoor hebben de medewerkers geen toestemming gegeven en is daarom een onrechtmatige verwerking.	M	L
M.6	Aanvraag voor medische hulpmiddelen op het werk bevatten de namen van betrokkenen. Het risico word ingeschat als laag omdat alleen de HR en eventueel ICT en/of FD hier toegang toe heeft. Daarnaast is het voor iedereen direct zichtbaar wanneer een dergelijk middel (zoals een aangepaste stoel) wordt gebruikt.	L	L
M.7	Facturen voor coaching bevatten namen van betrokkenen. Het risico word ingeschat als laag omdat alleen de financieel verantwoordelijke en Financiën hier toegang toe heeft.	L	L
M.8	Medewerkers zijn niet geïnformeerd over het gebruik van hun persoonsgegevens, waar deze zijn opgeslagen, etc. Ook zijn zij niet geïnformeerd welke rechten zij hebben en hoe ze deze kunnen uitoefenen binnen de No.	M	M

6.3 Overige

Risico	Beschrijving	Persoonlijke impact (L/M/H)	Business impact (L/M/H)
O.1	Oude camerabeelden van de bewakingscamera's worden automatisch gewist wanneer de harde schijf volloopt. Hierdoor worden de beelden mogelijk langer dan 28 dagen bewaard.	L	L
O.2	WieNo bevat contactgegevens van ministers, oud-medewerkers, ontvangers van jaarverslagen, en dergelijke. Deze gegevens zijn deels verouderd. De verouderde contactgegevens zijn gemarkeerd als 'inactief', maar worden bewaard.	L	L
O.3	Risico op tracking door Google Analytics.	M	L
O.4	Website bezoekers worden niet geïnformeerd over de mogelijkheid van tracking door social media wanneer zij op een facebook, twitter of linkedin-icoontje klikken.	M	L
O.5	Geen expliciete toestemming voor plaatsen (niet-functionele / tracking) third party cookies van Google Analytics op de website	M	L
O.6	Geen procedure voor vernietiging bezoekersregistratie. De impact als de registratie onbedoeld wordt gedeeld is echter minimaal. Wanneer iemand anoniem wil blijven, kan hij ervoor kiezen zijn naam niet te noemen.	L	L
O.7	Toestemming voor het gebruik van foto's van medewerkers en anderen in publicaties is niet vastgelegd. Hiermee voldoet de No niet aan haar verantwoordingsplicht.	L	M

7 Aanbevelingen om impact op privacy te verkleinen

Om de impact op privacy te verkleinen, worden de volgende maatregelen voorgesteld. Bij het uitwerken van de aanbevelingen, is eerst gekeken naar risico's met de hoogste impact op de betrokkene of de No.

7.1 Primair proces

Risico	Aanbeveling
P.1	Wijs aan individuele klachtendossiers een behandelaar en achtervang toe. Beperkt toegang tot de dossiers tot deze twee behandelaars. Organiseer een eenvoudig proces om rechten toe te kennen. Eventueel kan om aan de informatiebehoefte binnen teams te blijven voldoen, de herleidbare persoonsgegevens van de overige informatie in de dossiers worden gescheiden. Scherm de persoonsgegevens af voor niet-behandelaars. Voor structureel onderzoek kan een klein team toegang krijgen tot alle relevante informatie.
P.2	Maak klachtendossiers voor klachtbehandelaars onbeschikbaar nadat deze zijn afgesloten. Hanteer hierbij een nazorgtermijn van een jaar plus een maand. Verwijderen is niet mogelijk ivm structureel onderzoek en de levering aan het Nationaal archief. Een mogelijke oplossing is het verwijderen van toegangsrechten van klachtbehandelaars, waardoor de persoonsgegevens niet meer beschikbaar zijn in het primair proces (vgl. archiveren).
P.3	Informeer klagers over het beleid van de No om zo min mogelijk persoonsgegevens te verzamelen/bewaren over de klager, om het risico op onwenselijke verwerkingen en datalekken te voorkomen. Geef expliciet aan dat alle relevante stukken op basis van een wettelijke verplichting worden overgedragen aan het Nationaal Archief, waar deze voor o.a. historisch onderzoek ter inzage liggen. Neem deze informatie op in het Privacy Statement op de website.
P.4	Pas de bewaartermijn voor stukken mbt buitenwettelijke klachten aan naar drie maanden na afronding. Pas de selectielijst en de controle op de registratie hierop aan.
P.5	Stop met een aparte registratie van NAW-gegevens. Koppel deze gegevens aan een dossier.
P.6	Maak het mogelijk om het formulier anoniem in te dienen (zonder NAW of e-mailadres), of vermeld bij het formulier duidelijk een alternatieve wijze voor het indienen van een anonieme klacht (telefonisch).
P.8	De structurele aanpak is een wettelijke taak van de No. Hiervoor is geen toestemming benodigd. Wel moeten klagers worden geïnformeerd over dit gebruik. Hiervoor kan een informatieleaflet worden verstrekt aan het begin van de klachtbehandeling. In dit leaflet kunnen ook de overige over de verwerkingen, opslag, delen met derden en rechten van betrokkenen worden opgenomen. Als alternatief kan dit worden opgenomen in het privacy statement op de website.
P.9	Stel een richtlijn op waarin mobiel gebruik wordt toegestaan op voorwaarde dat de No het toestel op afstand mag wissen (incl. eventueel aanwezige privégegevens) bij een vermoedelijk datalek. Medewerkers moeten verlies,

Risico	Aanbeveling
	diefstal en een vermoedelijk datalek acuut melden. Richt technische maatregelen in waarmee het wissen op afstand door de No mogelijk is.
P.11	Stel een zeer compacte 'verwerkersovereenkomst' op (richtlijn: maximaal een A4tje) die voor uitwisseling met partijen kan worden ondertekend. Deze verwerkersovereenkomst moet het meest essentiële bevatten, afgestemd op uitwisselen van persoonsgegevens voor klachtbehandeling. O.a. het doel en de eis om gegevens te vernietigen na gebruik moeten hierin worden opgenomen. (Denk hierbij aan de wijze waarop geheimhoudingsverklaringen worden ondertekend tussen partijen die kortstondig vertrouwelijke gegevens delen).
P.12	Onderzoek of het mogelijk is om toegang tot de VIP-lijst te beperken. Bij voorkeur wordt het alleen mogelijk om individuele contactafspraken op te zoeken op naam of dossiernummer (bijv. tijdens het beantwoorden van een telefoongesprek). Het bekijken van de volledige lijst moet voorbehouden zijn aan enkele medewerkers die dit nodig hebben voor het beheer van de lijst. En richt een proces in om de gegevens niet onnodig lang te bewaren.
P.13	Uit nadere analys blijkt dat alleen dossiernummers en klachtomschrijving worden getoond in NoHow. NAW-gegevens zijn niet beschikbaar.
P.14	Implementeer een richtlijn waarin staat dat persoonsgegevens uitsluitend via Verseon mogen worden gedeeld. Verstuur geen persoonsgegevens via e-mail, maar deel links naar Verseon dossiers of deel dossiernummers. Hierdoor wordt ongeautoriseerd inzien (verwerken) voorkomen.
P.15	Richt een (cloud) portal in voor veilige bestandsuitwisseling van documenten met persoonsgegevens, zoals Citrix ShareFile. Maak hierbij gebruik van versleuteling om ongeautoriseerde toegang door de cloudleverancier te voorkomen. Als alternatief: versleutel alle bestanden met 7z of Zip met een wachtwoord dat via SMS of telefonisch wordt afgesproken.

7.2 Medewerkers

Risico	Aanbeveling
M.4	Breng deze gegevens onder in P-Direkt. Vernietig papieren dossiers en de bestanden op de G-schijf.
M.5	Informeer medewerkers dat het delen van privé-adressen door leidinggevenden en HR niet meer is toegestaan. Het registreren van toestemming kost te veel overhead. Adviseer medewerkers om onderling gegevens uit te wisselen indien zij prijs stellen op een kaartje.
M.8	Stel een informatieblad op voor medewerkers, waarin wordt toegelicht welke persoonsgegevens de No vastlegt, waarom, met welke grondslag, welke clouddiensten hierbij worden gebruikt, in welk geografisch gebied hun gegevens worden opgeslagen en hoe zij hun rechten (bijv. correctie, inzage) kunnen uitoefenen.

7.3 Overige

Risico	Aanbeveling
O.3	Beperk het delen van persoonsgegevens met Google. Kies voor de instelling om het laatste getal van het IP-adres niet te delen en kies de meest conservatieve analytics instelling mbt persoonsgegevens. Als alternatief: stop met Google Analytics en stap over op Pwik van de Rijksoverheid.
O.4	Informeer website bezoekers in het privacy statement over de mogelijkheid van tracking door social media wanneer zij op een facebook, twitter of linkedin-icoontje klikken.
O.5	Vraag expliciet om toestemming van de bezoeker voordat de website third party cookies van Google Analytics plaatst. Vervang Google Analytics door Piwik van de Rijksoverheid.
O.7	Doe een vrijwillige oproep aan medewerkers voor het verschijnen in foto's en leg de toestemming vast. Informeer medewerkers vooraf dat het intrekken van deze toestemming alleen effect heeft op toekomstige publicaties. Zorg ervoor dat bij het intrekken van deze toestemming, de foto's niet verder worden verwerkt in nieuwe publicaties.

8 Bijlage: overzicht verwerkingen

Deze PIA is gebaseerd op het overzicht van verwerkingen van 15 mei 2018.

8.1 Primair proces

Het onderstaand overzicht bevat de verwerkingen uit het register voor het primair proces. De verwerkingen die op basis van de uitkomsten van de PIA-workshops een PIA vereisen, zijn in het rood aangegeven.

1. **M3313 - Klachtbehandeling Veteranenombudsman**
2. **M1846 - Klachtbehandeling, en onderzoek uit eigen beweging, door de Nationale ombudsman**
3. **M2881 - Verwerken van AIVD documenten in Verseon**
4. **M2879 - Registreren van NAW gegevens in Verseon**
5. M3178 - het behandelen van inkomende en uitgaande post
6. M3281 - onderzoek uit eigen beweging door Nationale ombudsman
7. M1883 - Ontwikkelen en onderhouden lastig en complex klaaggedrag
8. M1896 - Post scannen
9. M1869 - Behandelen inzageverzoeken
10. M1927 - gebruik Coosto
11. M2080 - Rechten voor DOS en BI beheren
12. **M1902 - Klachtbehandeling kinderombudsman**
13. M1903 - Informatie ontsluiten op website over eigen organisatie
14. M1901 - Verstrekken van informatie aan de interne organisatie over de klachtbehandeling
15. M1899 - Het online uitnodigen van de Kinderombudsvrouw
16. **M1898 - Het online stellen van vragen aan de Kinderombudsman**
17. M1897 - Registratie van websitebezoeken

8.2 Bedrijfsvoering (medewerkers en overige)

Het onderstaand overzicht bevat de verwerkingen uit het register voor de bedrijfsvoeringsprocessen. De verwerkingen die op basis van de uitkomsten van de PIA-workshops een PIA vereisen, zijn in het rood aangegeven.

1. **M1859 - Personeelsgegevens P-direkt**
2. **M1882 - Volgen en beperken ziekteverzuim medewerkers**
3. **M1912 - Medewerkerstevredenheidsonderzoeken**
4. **M1880 - Uitvoeren bovenwettelijke regelingen**
5. **M1863 - Gebruikmaken van openbaarvervoer kaarten**
6. **M1893 - Het houden van cameratoezicht**
7. **M2882 - Onderhouden relaties in WieNo**
8. **M2387 - Google Analytics**
9. M3451 - Vodafone gebruikers
10. M1870 - Inzichtelijk maken van opleidingen
11. M1890 - Inzicht en beoordelen nevenfuncties
12. M1864 - Het managen van de processen medewerker in- en uit dienst

13. M3442 - Auditlogs IT Infrastructuur
14. M1868 - Aanvragen ARBO middelen
15. M1873 - Uitvoeren bezwaar en beroepsprocedures en advies rechtspositie
16. M1858 - Bijhouden geschenkenregister
- 17. M1877 - Uitvoeren werving en selectietrajecten personeel met dienstverband en externe inhuur**
18. M2511 - Windows domein account medewerker
19. M3264 - Beheer archieven No door Nationaal archief
20. M2888 - Bezoeker registratie
- 21. M3305 - Vastleggen medische achtergrond No medewerkers**
22. M3307 - Vastleggen deelnemers BHV
23. M3304 - Aanvragen parkeerplaatsen
24. M1894 - Toegangscontrole van medewerkers
- ~~25. M1895 - Reserveren van facilitaire diensten (dubbel)~~
26. M3268 - Registratie kentekens No medewerkers
27. M1892 - Het gebruiken van Multifunctionals
- ~~**28. M3220 - Aanvragen, beheren en onderhouden registratienummer medewerker (RIN) (dubbel)**~~
29. M3376 - Registreren van beveiligingsincidenten
30. M1875 - Uitvoeren van audits, onderzoeken en interne controle op interne organisatie
31. M1879 - Toegang tot goedkoper sporten
- ~~32. M3177 - Integriteit bewaken en volgen → vervalt~~
33. M1884 - Het voeren van deugdelijk materieel beheer
34. M1887 - Beheersen van projecten en activiteiten met Trello
- 35. M1862 - Behandelen interne klachten**
36. M1876 - Uitzetten enquêtes en vragen van feedback
37. M2793 - Contactgegevens intern + extern
38. M2583 - TOPdesk (kennisbank)
39. M2572 - NoHow - intranet
40. M1921 - Ontsluiten informatie op website No en Kom over eigen organisatie
41. M3300 - Bibliotheek BNo - JouwNieuws
42. M1905 - Voeren financiële administratie
43. M3214 - Verstrekken van financiële managementinformatie
44. M3286 - Uitvoeren en contractbeheer van de inkoop van goederen en diensten
45. M2577 - Bibis
46. M2794 - Inloggegevens
47. M3229 - Uitvoeren EU aanbestedingen (Tendered)
48. M1885 - Rapportage over de inkoop van de organisatie d.m.v. een Spendanalyse
49. M3213 - Uitvoeren betalingen via internetbankieren
50. M3221 - Betalingen verrichten met creditcard
51. M2382 - Online contactformulier
52. M2379 - Online klachtenformulier
53. M1881 - Het boeken van buitenlandse dienstreizen
54. M1916 - Het online mogelijk maken van het toesturen van folders en brochures

- 55. M2388 - Online rapporten, onderzoeken en dossiers
- 56. M2786 - Verslagen van overleggen/vergaderingen
- 57. ~~M2581 - Aangevraagde en toegestuurde offertes (dubbel)~~
- 58. M1919 - Ontsluiten rapporten en andere informatie rondom klachtbehandeling
- 59. M2385 - Video's Social media kanalen
- 60. M1871 - Inventariseren integriteitsschendingen**
- 61. M1918 - Ombudskalender
- 62. M1926 – Onderhouden medewerkergegevens op Rijksportaal
- 63. M2900 - Nieuwsbrieven**

Rapport

Status implementatie AVG bij de Nationale ombudsman

1	Inleiding	30
1.1	Doel van dit document	30
1.2	Opbouw van dit document	30
2	Status	31
2.1	Bewustwording	31
2.2	Rechten van betrokkenen	32
2.3	Overzicht van verwerkingen	32
2.4	Data Protection Impact Assessment	33
2.5	Privacy by Design & Privacy by Default	33
2.6	Functionaris Gegevensbescherming	34
2.7	Meldplicht datalekken	34
2.8	Verwerkingsovereenkomsten	34
2.9	Toestemming	35
3	Planning	36
4	Aandachtspunten	37
4.1	Registratie BSN nummer	37
4.2	Registratie NAW gegevens	37
4.3	Archiefwet vs. AVG	37
4.4	Gebruik Google Analytics op de website	37
4.5	Caribisch Nederland/landen buiten AVG-gebied	37

9 Inleiding

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Deze verordening vervangt de Wet bescherming persoonsgegevens (WBP).

De AVG versterkt de positie van betrokkenen. Zij krijgen nieuwe privacy rechten en hun bestaande rechten worden sterker. De organisaties, zoals de Nationale ombudsman (No), die de persoonsgegevens verwerken krijgen meer verplichtingen. Organisaties worden verantwoordelijk voor het kunnen aantonen dat ze zich aan de wet houden.

9.1 Doel van dit document

Het doel van dit document is om de directeur van de No, tevens de verwerkingsverantwoordelijke, te informeren over de status van de implementatie van de AVG op 25 mei 2018.

9.2 Opbouw van dit document

De Autoriteit Persoonsgegevens (AP) heeft een 10 stappen plan ontwikkeld voor de implementatie van de AVG. In hoofdstuk 2 wordt aan de hand van dit stappenplan beschreven hoe ver de No is met de implementatie.

In hoofdstuk 3 wordt een planning gegeven van activiteiten die in de komende periode moeten worden uitgevoerd om de AVG implementatie volledig te maken.

Hoofdstuk 4 tot slot beschrijft een aantal aandachtspunten dat tijdens het implementatie traject zijn signaleerd en aandacht behoeven.

10 Status

De Autoriteit Persoonsgegevens heeft in een 10 stappenplan de belangrijkste elementen ter voorbereiding van 25 mei opgenomen. Deze stappen worden in dit hoofdstuk gebruikt om aan te geven hoever de implementatie daarvan is bij de No. De stap 'Leidende toezichthouder' is niet van toepassing voor de No en wordt buiten beschouwing gelaten.

Per stap wordt met een kleur de status van de implementatie aangegeven.

	Aan deze stap is helemaal voldaan
	Aan deze stap is grotendeels voldaan en wordt op korte termijn afgerond
	Aan deze stap is nog niet of minimaal voldaan

10.1 Bewustwording

Deze stap richt zich op de interne organisatie. De relevante mensen in de organisatie moeten op de hoogte van zijn de nieuwe privacyregels.

In het kader van de bewustwording zijn de volgende acties ondernomen:

Training over de AVG voor de hele organisatie

Status	Ingepland nog niet uitgevoerd
--------	-------------------------------

Er wordt met behulp van een deskundig bureau een training over de AVG samengesteld voor alle medewerkers. Deze of een gelijksoortige training zal vervolgens structureel georganiseerd gaan worden voor nieuwe medewerkers als onderdeel van het inwerkprogramma. De training is verplicht.

Het bureau wat de training gaat verzorgen is geselecteerd en de data voor de trainingen worden gepland in de maand juni en begin juli.

De training zal in inhoud verschillen naargelang de doelgroep;

- Primair Proces en omgevingsmanagement
- FD en Secretariaat
- Communicatie en Bestuursbureau

Verhoogde communicatie over de AVG op NoHow

Status	Doorlopend proces
--------	-------------------

De organisatie wordt via NoHow frequenter op de hoogte gebracht van zaken over de AVG. Voorbeelden hiervan zijn berichtgeving over Datalekken en hoe deze te voorkomen, het veilig vaststellen van bijlagen met 7zip en hoe om te gaan met toestemming in geval van gebruik foto's.

Activeren van AVG expertise groep

Status	Afgerond
--------	----------

Ter ondersteuning van de FG is er een AVG expertise groep samengesteld. Deze groep bestaat uit medewerkers uit verschillende geledingen in de organisatie (FD, Bestuursbureau, Communicatie en omgevingsmanagement, primair proces en Kinderombudsman). De expertise groep zorgt er voor dat de AVG een actueel item blijft binnen de verschillende afdelingen, functioneert als vraagbaak voor de organisatie en beheert de verwerkingen van persoonsgegevens in het AVG register.

Training voor de AVG expertise groep

Status	Ingepland, nog niet uitgevoerd
--------	--------------------------------

Er wordt specifiek voor de AVG expertise groep een diepgaande training georganiseerd. Deze training heeft een duur van 2 dagen waarbij de eerste dag voornamelijk theoretisch van aard zal zijn en de tweede dag gebruikt wordt voor het behandelen van situaties specifiek voor de Nationale ombudsman. Deze training is ingepland in de maand juni.

Handboek AVG

Status	In opzet, verzamelen van inhoud
--------	---------------------------------

Er wordt een handreiking samengesteld met tips en trucs, vragen en antwoorden en wetenswaardigheden over de AVG en hoe deze toe te passen.

Dit handboek wordt in de kennisbank gepubliceerd en tevens op NoHow ontsloten.

10.2 Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie wij persoonsgegevens verwerken meer en verbeterde privacy rechten.

Privacy statement op website Nationale ombudsman

Status	Initiële versie afgerond
--------	--------------------------

Op de website van de No en de Kom staat een privacy verklaring waarin wordt toegelicht hoe er met persoonsgegevens van burgers wordt omgegaan. Deze privacy verklaring is aangepast zodat het in lijn is met de AVG. De rechten van betrokkenen zijn toegelicht en de contactmogelijkheid met de FG van de No is vermeld. Hoewel de privacy verklaring online is wordt deze nog wel verder aangescherpt de komende tijd.

Interne procedure rechten van betrokkenen

Status	10% afgerond
--------	--------------

De AVG geeft de burger meer rechten. Dit betekent dat er intern een duidelijke procedure moet worden opgesteld hoe om te gaan met verzoeken van burgers waarbij ze gebruik maken van deze rechten.

Het gaat hierbij om;

1. Recht op informatie
2. Recht op rectificatie
3. Recht op beperking van de verwerking
4. Recht van bezwaar
5. Recht om vergeten te worden en
6. Recht op inzage

In deze procedure wordt beschreven hoe verzoeken worden behandeld en geregistreerd. Maar ook waar de verzoeken opgeslagen worden en hoe lang de gegevens bewaard blijven. Deze procedure moet nog in detail worden uitgewerkt.

10.3 Overzicht van verwerkingen

Status	80% afgerond
--------	--------------

Alle gegevensverwerkingen moeten in kaart gebracht worden. Hierbij moet worden vastgelegd welke persoonsgegevens worden verwerkt, met welk doel, waar de gegevens vandaan komen, hoe de persoonsgegevens beveiligd zijn en met wie we ze delen. Met behulp van deze registratie kunnen we aantonen dat we in overeenstemming met de AVG handelen.

We maken gebruik van een online AVG registertool van het Ministerie van Economische zaken.

Op dit moment zijn er 78 verwerkingen geregistreerd. De verwerkingen zijn opgesplitst naar organisatie onderdeel/afdeling.

Aan elke verwerking is een contactpersoon toegekend. Deze contactpersoon is verantwoordelijk voor het actueel houden van de verwerking.

Onderdeel	Aantal verwerkingen	In bewerking	Af of in review
-----------	---------------------	--------------	-----------------

Bestuursbureau	32	5	27
Communicatie & Omgevingsmanagement	13	10	3
Facilitaire Dienst	15	1	14
ICT	4	2	2
Kinderombudsman	6	6	0
Sectoren No	4	3	1
Veteranenombudsman	1	0	1

Hoewel alle verwerkingen geregistreerd zijn is ongeveer de helft nog in bewerking. De andere helft is in concept of aangeboden ter review.

10.4 Data Protection Impact Assessment

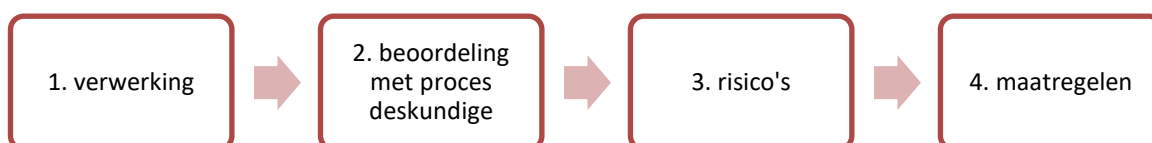
Status	PIA sessies uitgevoerd, maatregelen nog uitwerken en implementeren
---------------	---

Verwerkingen die een hoog risico voor de privacy van betrokkenen hebben, moeten in detail uitgewerkt worden in een zogeheten Data Protection Impact Assessment (DPIA). Met dit instrument worden de risico's van een verwerking in kaart gebracht en kunnen vervolgens maatregelen opgesteld en uitgevoerd worden om de risico's te verkleinen.

Bij het vullen van het verwerkingen register bepaalt het programma door het stellen van vragen voor welke verwerkingen een DPIA moet worden uitgevoerd.

Er zijn zowel in het primaire proces als in de bedrijfsondersteuning een aantal verwerkingen geregistreerd waarvoor een PIA moet worden uitgevoerd.

Het proces van een PIA is globaal als volgt:



1. er wordt voor een verwerking geconstateerd dat een PIA nodig is.
2. de verwerking wordt met proces/verwerkingsdeskundigen geanalyseerd.
3. Hierbij worden alle risico's in kaart gebracht.
4. Tot slot worden maatregelen gedefinieerd en geïmplementeerd om de risico's te minimaliseren.

Op dit moment is voor die verwerkingen waar een PIA op van toepassing was, stap 1 t/m 3 uitgevoerd. Stap 4 is gaande.

10.5 Privacy by Design & Privacy by Default

Privacy by Design en Privacy by Default zijn onder de AVG verplichte uitgangspunten.

Privacy by Design houdt in dat er bij het ontwerpen van producten en diensten wordt gezorgd dat persoonsgegevens goed worden beschermd.

Privacy by Default houdt in dat er technische en organisatorische maatregelen worden genomen om er voor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel wat we willen bereiken.

Voor beide punten geldt dat de organisatie vertrouwd raakt met deze uitgangspunten en dat nog verder onderzocht moet worden hoe deze beginselen binnen de organisatie worden ingevoerd.

Bewustwording Privacy by design

Status	Doorlopend proces
---------------	--------------------------

Binnen de organisatie moet de bewustwording worden gecreëerd dat bij elk nieuw product of dienst wat wordt afgenomen of ontwikkeld de FG betrokken moet zijn om te controleren of

het product of dienst in overeenstemming is met de AVG. De AVG vertegenwoordigers in elk team/afdeling spelen een belangrijke rol hierin. Er wordt nog verder gekeken naar aanvullende maatregelen.

BIR

Status	In behandeling
---------------	-----------------------

Eind 2017, begin 2018 is er door de Auditdienst Rijk (ADR) een nulmeting van de Informatiebeveiliging bij de No uitgevoerd a.d.h.v. de Baseline informatiebeveiliging Rijksdienst (BIR-2012). Dit heeft een rapport opgeleverd waarin een aantal aanbevelingen zijn opgenomen om de informatiebeveiliging te optimaliseren. Deze aanbevelingen worden gedurende het project locatie onafhankelijk werken en deels volgend jaar opgevolgd. Hierna voldoet de No aan de BIR-2012.

Vernieuwing Oracle omgeving

Status	In behandeling
---------------	-----------------------

Eind 2017 is een analyse uitgevoerd op de Oracle omgeving (BI, DOS, Verseon Database, Reports). Hierbij is onder andere gekeken naar de huidige staat van toegepaste security patching en support status van de verschillende Oracle componenten. Dit onderzoek heeft een scenario opgeleverd waarbij alle Oracle componenten naar een versie worden gebracht waarin ze binnen de support cyclus van Oracle vallen en daarnaast worden alle componenten gepatched met de meest actuele security updates. Het bijwerken van de security patches wordt vervolgens een periodieke actie. Het vernieuwen van de Oracle omgeving zal in Q3 en Q4 van 2018 worden uitgevoerd.

10.6 Functionaris Gegevensbescherming

Status	afgerond
---------------	-----------------

De No is verplicht om een Functionaris Gegevensbescherming (FG) aan te stellen. Dit is gebeurd en per 23 april is de OR akkoord gegaan met de benoeming.

De Functionaris Gegevensbescherming is de contactpersoon voor de Autoriteit Persoonsgegevens en bewaakt tevens de implementatie en uitvoering van de AVG binnen de organisatie.

In afwezigheid van de FG is de AVG-groep het aanspreekpunt voor vragen en verzoeken m.b.t. AVG. Het bestuursbureau neemt in afwezigheid procedurele taken over zoals het afhandelen van datalekken.

10.7 Meldplicht datalekken

Status	afgerond
---------------	-----------------

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. Er worden wel strengere eisen gesteld aan de registratie van de datalekken.

Bij een datalek wordt een melding gemaakt in Topdesk en een datalek registratie formulier wordt door de melder ingevuld. De FG beoordeelt of het om een datalek gaat. Is dat het geval dan wordt beoordeeld of de aard van het lek dermate ernstig is dat het aan het AP (en eventueel aan de betrokkene) moet worden gemeld of dat het zonder melding afgehandeld kan worden.

In BureauDok wordt een dossier aangelegd van elk Datalek waarin alle stukken worden bewaard.

Het proces datalekken is volledig geïmplementeerd en gecontroleerd of het in overeenstemming is met de AVG.

10.8 Verwerkingsovereenkomsten

Status	90% afgehandeld
---------------	------------------------

Wanneer we gegevensverwerking hebben uitbesteed aan een verwerker, moet worden beoordeeld of de overeengekomen maatregelen in bestaande contracten met de verwerkers

toereikend zijn en of ze voldoen aan de eisen die de AVG stelt aan verwerkingsovereenkomsten.

We hanteren bij voorkeur de ARVODI overeenkomst voor verwerkers.

Een aantal verwerkers hebben een eigen overeenkomst. Deze wordt beoordeeld op technische en juridische inhoud en indien deze gelijkwaardig of beter wordt bevonden dan de ARVODI overeenkomst, wordt deze gehanteerd.

Met 90% van de verwerkers is ondertussen een verwerkingsovereenkomst gesloten.

10.9 Toestemming

Status	In behandeling
--------	----------------

Voor sommige gegevensverwerkingen is toestemming nodig van betrokkenen. De AVG stelt strengere eisen aan toestemming.

Er wordt in kaart gebracht voor welke verwerkingen toestemming van betrokkenen nodig is en tevens hoe een toestemming vastgelegd moet worden en waar.

11 Planning

Hoewel er de afgelopen periode veel werk is verzet om de implementatie van de AVG voor 25 mei zo veel mogelijk te realiseren, zijn er nog veel activiteiten over waar de komende periode aan gewerkt moet worden.

De planning voor dit jaar is opgenomen in een aparte bijlage 'PO planning.pdf'.

In deze planning zijn de activiteiten ingedeeld in de stappen uit het 10 stappen plan van het AP.

12 Aandachtspunten

Gedurende de afgelopen maanden waarin de AVG implementatie binnen de No in een stroomversnelling is beland, zijn een aantal zaken naar voren gekomen die nader onderzoek vereisen en mogelijk tot een advies of wijziging kunnen leiden.

12.1 Registratie BSN nummer

Verseon biedt de mogelijkheid om het BSN nummer te registreren bij een NAW.

Bij navraag blijkt dat het BSN nummer niet of nauwelijks gebruikt wordt bij behandeling van een dossier. Het BSN nummer is vaak opgenomen in een dossierstuk en wordt op die manier meegegeven aan bijvoorbeeld het UWV of de Belastingdienst.

In het kader van dataminimalisatie is het wenselijk om het veld BSN te verwijderen uit Verseon.

12.2 Registratie NAW gegevens

De afgelopen maanden zijn er een aantal datalekken geweest. In vrijwel alle gevallen gaat het om het versturen van gegevens naar een verkeerde afzender. Het is ook voorgekomen dat een afzender niet langer woonachtig was op het adres wat in Verseon geregistreerd staat.

Een manier om dit soort fouten tot een minimum te beperken is door NAW's niet als losse entiteiten te registreren en deze vervolgens te koppelen aan een dossier, maar door de NAW registratie binnen een dossier te doen. Dit heeft als gevolg dat een verzoeker meerdere keren in het systeem kan voorkomen en het uniek identificeren van een verzoeker lastiger wordt.

Er is nader onderzoek nodig om te bepalen wat de voor- en nadelen van een dergelijke implementatie zijn en welk belang zwaarder weegt.

12.3 Archiefwet vs. AVG

De afgelopen maanden is regelmatig de vraag opgekomen hoe de AVG en de Archiefwet zich verhouden tot elkaar.

In de notitie 'Verhouding AVG – Archiefwet' wordt hierop ingegaan.

Hier zijn een aantal punten met adviezen naar voren en deze zijn in het Corporate Overleg (CO) besproken. :

1. Geen verzoeken de kenbaarheid in sturen zonder toestemming van de verzoeker
2. Standaard werkwijze opstellen voor het vragen van toestemming
3. Uitzoeken juiste werkwijze t.a.v. het vernietigen van NAW gegevens
4. Bewaartermijnen in het basis selectie document opnieuw bekijken
5. Op de website verzoekers informeren om zo min mogelijk stukken in te sturen.

CO is akkoord met de adviezen. Deze moeten nu worden opgepakt en geïmplementeerd.

12.4 Gebruik Google Analytics op de website

Voor bezoeksmetingen op de website van de No en Kom wordt Google Analytics gebruikt. De data van deze metingen wordt op servers van Google opgeslagen en door Google gebruikt voor analyses.

Piwik Analytics is een alternatief wat veel binnen de overheid wordt gebruikt. Piwik voldoet aan de AVG en werkt alleen met anonieme, geaggregeerde bezoekstatistieken die niet herleidbaar zijn naar een persoon.

Er wordt onderzocht of een overstap van Google Analytics naar Piwik Analytics mogelijk is en zal t.z.t. als advies worden aangeboden.

12.5 Caribisch Nederland/landen buiten AVG-gebied

De No is bevoegd over de Caribisch Nederlandse overheid die op Aruba, Sint Maarten of Curaçao zetelt en over buitenlandse overheid die soms optreedt als Caribisch Nederlandse

overheid (denk aan een Sint Maartense deurwaarder die op Saba of Sint Eustatius beslag legt). Wij wisselen gegevens uit met deze overheden.

Daarnaast wisselen wij bij de klachtbehandeling gegevens uit met verzoekers die buiten AVG-gebied wonen en die klagen over Nederlandse of Caribisch Nederlandse overheidsinstanties.

Vaak is de AVG dan niet volledig van toepassing; wel op ons maar niet voor bijvoorbeeld op Caribisch Nederland. Het gevolg hiervan is dat wij dan voor passende waarborgen moeten zorgen bij gegevensuitwisseling.

Eén en ander is inmiddels in kaart gebracht, maar het is nog niet voldoende duidelijk wat dit voor ons en onze contacten met dergelijke instanties betekent. Het wachten is op een nieuwe Guideline van de Europese Commissie die binnenkort zal verschijnen; de verwachting is dat deze meer duidelijkheid verschaft.

Ook kan overwogen worden een vraag hierover bij de AP uit te zetten.



Document classificatie

Vertrouwelijk

Versiebeheer

Versienummer	1.0 DEFINITIEF
Opgesteld door	 J
Datum eerste versie	18 september 2020
Laatst bijgewerkt	17 september 2021
Bron van het document	Informatiebeveiligingsdienst (IBD)

Geschiedenis wijzigingen

Versienr.	Datum	Auteur	wijzigingen
0.2	25-9-2020	 J	Omgeschreven naar No
0.3	07-10-2020	 J	
0.4	8-10-2020	 J	
0.5	23-10-2020	 J	Procedure melding datalek buiten incidentmanagement
0.6	05-11-2020	 J  J	
0.7	13-11-2020	 J	
0.8	29-01-2021	 J	Versie na eerste evaluatie

0.9	23-06-2021	 J	Versie na workshop werkinstructie incidentmanagement
0.9.2	23-07-2021	 J	Review op basis van gemaakte aanpassingen.
0.9.3	30-7-2021	 J	Update op basis van gezamenlijke review
0.95	3-08-2021	 J	Gegevens in bijlage 3 geupdate. Nog finaliseren voor versie BVO
1.0	17-9-2021	 J	Versie vastgesteld in BVO

Inhoud

1	Inleiding	1
1.1	Beschikbaarheid, Integriteit en Vertrouwelijkheid	1
1.2	Doelstelling incidentmanagement	1
2	Incidentmanagement en response stappen	3
2.1	Definities	3
2.2	Personeel	3
2.3	Opzetten incidentmanagement	5
2.3.1	Identificatie	5
2.3.2	Schade indamming	5
2.3.3	Remediatie en herstel	6
2.3.4	Kennisgeving	6
2.3.5	Rapportage en evaluatie	6
2.4	Hoe te gebruiken?	6
3	Aandachtspunten	8
3.1	Logging	8
3.2	Vorbereiding	8
3.3	Gouden uur	8
3.3.1	Gouden tips	9
4	Incident Prioritering Leidraad	10
4.1	Incident urgentie	10
4.2	Incident impact (categorieën)	11
4.3	Incident Prioriteringsklassen	12

4.3.1	Omstandigheden die het noodzakelijk maken dat een incident behandeld wordt als een groot incident.....	12
4.3.2	Indicatoren	13
4.3.3	Het identificeren van kritische incidenten	13
4.3.4	Belangrijkste eigenschappen van kritische incidenten.....	13
Bijlage 1: Major & Security incident stappenplan		15
Bijlage 2: Minor incident stappenplan		26
Bijlage 3: Checklist Incident response		28

1 Inleiding

Incidentmanagement bevat het identificeren, oplossen en het leren van een incident, zodat de impact en kans op herhaling minimaal is. Het gaat bij informatiebeveiliging om informatiebeveiligingsincidenten die betrekking hebben op de informatievoorziening. Het primaire doel is de ontwikkeling van een goed begrepen en voorspelbare reactie op schadelijke gebeurtenissen in de meest brede zin van het woord. De wijze waarop een datalek wordt gemeld en vervolgens afgehandeld valt buiten de scope van deze beschrijving, tenzij tijdens de behandeling van een incident wordt vastgesteld dat het incident ook heeft geleid tot een datalek. In dat geval wordt de FG hiervan op de hoogte gesteld en zal de FG het datalek verder in behandeling nemen.

De Nationale ombudsman moet zich bewust zijn van de verantwoordelijkheden als het gaat om de bescherming van informatie ten behoeve van de burgers en (Rijks)overheid. Deze verantwoordelijkheid strekt zich uit tot het hebben van een draaiboek voor 'wat te doen, als er iets misgaat'.

1.1 Beschikbaarheid, Integriteit en Vertrouwelijkheid

Incidentmanagement is een belangrijk onderdeel van informatiebeveiliging. Niet alle incidenten die kunnen plaatsvinden binnen een organisatie zijn echter informatiebeveiligingsincidenten. Maar, toch is dit heel vaak wel het geval. Informatiebeveiliging gaat over het waarborgen van de volgende drie aspecten:

- **Beschikbaarheid** beschrijft de beschikbaarheidsvereisten ten aanzien van de data die wordt gebruikt.
- **Integriteit** betreft de juistheid en volledigheid van de data die gebruikt wordt.
- **Vertrouwelijkheid** geeft aan wie toegang tot de data mag hebben en welke bevoegdheden hieraan gekoppeld zijn. (Bijvoorbeeld muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie)

Hieruit blijkt dat informatie dus niet alleen beveiligd moet worden tegen actoren met een kwade intentie van binnen of buiten een organisatie. Ook incidenten zoals het niet opzettelijk wissen van gegevens, of een storing in het energienet of in een serverruimte gaan dus over informatiebeveiliging. Informatie is dan namelijk (tijdelijk) niet beschikbaar. Deze incidenten dienen dus ook als informatiebeveiligingsincidenten te worden behandeld.

1.2 Doelstelling incidentmanagement

Incidentmanagement is zo belangrijk omdat 100% beveiligen niet bestaat en los daarvan: niet alle incidenten zijn te voorkomen. Het is niet de vraag óf er iets gaat gebeuren maar wanneer. De belangrijkste te verwachte incidenten kunnen van te voren bedacht worden en de

bijpassende reactie en escalatieprocedure kan dus ook van te voren uitgewerkt en geoefend worden. Het incidentmanagementproces heeft dan ook als doel om ongeplande serviceonderbrekingen zo snel mogelijk te verhelpen.

Incidenten staan vaak niet op zichzelf en kunnen een uitwerking hebben naar andere belanghebbenden. Een incident moet behalve intern opgelost soms ook extern geëscaleerd worden zodat anderen gewaarschuwd kunnen worden en daarmee de impact van het incident zo klein als mogelijk gehouden kan worden. Extern escaleren gebeurt naar Ilionx. Indien nodig kunnen we ook escaleren richting het Nationaal Cyber Security Centrum (NCSC), zij hebben als Computer Emergency Response Team (CERT) het overzicht, de contacten en de middelen om andere overheden snel te kunnen waarschuwen.

2 Incidentmanagement en response stappen

Een incident, in het kader van incidentmanagement, is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentmanagement is het geheel van organisatorische maatregelen dat ervoor moet zorgen dat een incident adequaat gedetecteerd, gemeld en behandeld wordt om daarmee de kans op uitval van bedrijfsvoering processen of schade ontstaan als gevolg van het incident te minimaliseren, dan wel te voorkomen.

2.1 Definities

Minor incident: Een minor incident heeft geen invloed op cruciale onderdelen van het systeem en zal ook niet eisen dat er extra controles moeten worden uitgevoerd. Minor incidenten vereisen geen interventie van hoger personeel of het management en er is geen melding van het event vereist.

Major incident: Een major incident treft kritische productiesysteem of -systemen, heeft verregaande gevolgen voor grote delen van de informatievoorziening en vereist dat er maatregelen genomen moeten worden om mogelijke gevolgen in te perken en verdere schade, dan wel uitval, te voorkomen van dat systeem of deze systemen. Major incidenten vereisen onmiddellijk handelen en de deelname van hoger personeel en het informeren van belanghebbenden zoals systeemeigenaren, leidinggevenden en het Response team.

Security incident: Een security incident is een verstoring die impact heeft op de dienstverlening, dit kan betrekking hebben op de beschikbaarheid van systemen of informatie) en/of het ongeoorloofd openbaren, verkrijgen en/of wijzigen van informatie (vertrouwelijkheid of integriteit van informatie of systemen). Een security incident kan zowel een Minor als Major incident zijn.

Privacy incident: Een security incident waarbij er toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens heeft plaatsgevonden, zonder dat dit de bedoeling was van de No. Een Privacy incident kan zowel een Minor als Major incident zijn.

2.2 Personeel

Het incidentmanagementproces moet een eigenaar hebben en binnen het proces moet een vast aanspreekpunt zijn die eventueel ook zorgdraagt voor de externe communicatie. Het melden van incidenten is een taak van iedereen. De beoordeling van de logging maar ook van gemelde incidenten behoort door een speciaal aangewezen functionaris te gebeuren

afhankelijk van waarover de logging of de incidentmelding gaat. In ieder geval moet altijd de servicedesk geïnformeerd worden. Onrechtmatigheden van een bepaalde categorie moeten gemeld worden aan de Chief Information Security Officer (CISO). Bij een escalatie of een noodsituatie moet altijd rekening gehouden worden met woordvoering waarbij Ilionx of eventueel het Nationaal Cyber Security Centrum (NCSC) advies kan geven. Al het personeel dat betrokken is bij het incidentproces moet op de hoogte zijn van de procedures en de telefonische bereikbaarheid van belangrijke contactpersonen en teamleden. Per soort incident kan het team een wisselende samenstelling hebben. Onderstaand overzicht beschrijft de belangrijkste functionarissen bij een incident. Contactgegevens van de functionarissen en die van de betrokken leveranciers zijn beschreven in de checklist (zie bijlage 3). Deze checklist is offline en in hardcopy beschikbaar.

Stakeholder	Verantwoordelijkheid	Functionaris	Indien niet beschikbaar
Incident-manager	Beheren van het incidentmanagementproces en verantwoordelijk voor de communicatie binnen en eventueel buiten de No	Hoofd FD	Hoofd Bestuursbureau
Systeem-beheerder	Verzamelen van technische informatie en incident informatie	Systeembeheerder	Systeembeheerder
Helpdesk ICT	Verzamelen van technische informatie en incident informatie	Helpdesk ICT	Hoofd FD
CISO	Beoordelen en begeleiden van incidenten m.b.t inbreuk op de beschikbaarheid (>2uur) integriteit en vertrouwelijkheid.	CISO	FG
FG	Beoordelen en begeleiden van incidenten die tot een datalek kunnen of hebben geleid.	FG	CISO
Cyber Response leverancier	Verantwoordelijk voor het verzamelen en beschermen van bewijsmateriaal. Indien nodig ook voor het geven van advies m.b.t een incident.	Informatiebeveiliging advies (extern)	NCSC
MT-aanspreekpunt	Verantwoordelijk voor de communicatie naar het MT	Hoofd Bestuursbureau	Hoofd Communicatie en Omgevingsmanagement

	en bevoegd om beslissingen te nemen.		
--	---	--	--

2.3 Opzetten incidentmanagement

Een succesvol incidentmanagement- en responsebeleidsreactie bestaat uit een aantal te doorlopen stappen. Deze stappen zijn voor ieder incident gelijk, alleen in de details zitten de verschillen.

De volgende informatie is bedoeld als een algemene checklist van de stappen die de No kan nemen wanneer een incident wordt ontdekt. Er bestaan andere checklists en deze kunnen ook al in gebruik zijn. Deze checklist kan nuttig zijn voor iedereen, als een herziening van paraatheid of als een routekaart voor ontwikkeling. De eigenaar van het incidentmanagement- en responseproces is de incidentmanager. De helpdesk heeft een nadrukkelijke rol bij het ontwikkelen van incidentresponsereacties en bij de voorbereiding daarop.

Belangrijk is dat incidenten en uitgevoerde activiteiten worden vastgelegd voor latere evaluatie, woordvoering, bewijslast en dergelijke.

Een incident response-actie bestaat uit de volgende stappen:

- 1) identificatie;
- 2) schade indamming (insluiting en beperking);
- 3) remediatie en herstel;
- 4) kennisgeving, en;
- 5) rapportage en evaluatie.

2.3.1 Identificatie

Controleer of er een kwetsbaarheid aanwezig is en/of een incident daadwerkelijk heeft plaatsgevonden en registreer het incident.¹ Deze activiteit omvat normaliter de systeembeheerder en eindgebruiker, maar kan ook het gevolg zijn van proactieve detectie van incidenten door de ICT-beveiliging of het systeembeheer of doordat bij de controle van de logging of via signalering door de monitoringsystemen iets naar boven komt.

2.3.2 Schade indamming

Nadat het incident is opgemerkt en gemeld gaat de ICT-helpdesk ermee aan de slag. De helpdeskmedewerker moet in het geval van een klein incident gaan handelen om de schade van het incident te beperken. Indien het incident groter is betreft de helpdeskmedewerker de incidentmanager. De incidentmanager zal waar nodig een team aanstellen om het incident te

¹ Registratie van het incident vindt plaats in TopDesk.

verhelpen en zal hiervoor soms ook de CISO & FG nodig hebben. Bij grote informatiebeveiligingsincidenten zal de manager Bestuursbureau een belangrijke rol spelen en zal de CISO in de meeste gevallen de teamleider worden. Dit team is belast met het beperken van verdere schade als gevolg van het incident en kan Ilionx of eventueel het NCSC inschakelen voor advies.

Start een grondige beoordeling van de aard en omvang van het incident, stel vast wat de schade is en stel bewijsmateriaal veilig. Volg indien er gegevens zijn gelekt het datalekkenproces.

2.3.3 Remediatie en herstel

Neem maatregelen om de oorzaak van het incident te blokkeren of te verwijderen, verminder de impact door verdere blootstelling van de gevoelige gegevens te voorkomen, maak een start om de bedrijfsprocessen te herstarten als deze gestopt waren als gevolg van het incident en zorg ervoor dat risico's die verband houden met dit incident worden gemitigeerd. Als er diensten zijn uitbesteed is het noodzakelijk om goede afspraken te maken met de leverancier om incidenten goed op te pakken.

2.3.4 Kennisgeving

Bepaal welke gegevens mogelijk zijn blootgesteld door het incident en stel de getroffen en in kennis van het feit dat hun gegevens blootgesteld zijn. Informeer indien noodzakelijk andere overheidsinstanties, zoals het NCSC en/of de politie. Betrek voor deze melding eventueel een jurist. Snelheid is ook belangrijk vanuit een PR-oogpunt. Afhankelijk van de aard van het incident kunnen sommige stappen parallel uitgevoerd worden. Let op, het is ook raadzaam om bij de woordvoering over een incident een jurist te betrekken, de aard en inhoud van de communicatie kan gevolgen hebben voor aansprakelijkheid van de Nationale ombudsman.

2.3.5 Rapportage en evaluatie

Identificeer lessen uit het incident en bespreek deze met het team, rapporteer over het incident, de genomen maatregelen en het algemeen verslag, rapporteer indien nodig intern en extern, pas het gevolgde draaiboek aan. Incidenten moeten goed worden opgeschreven, met de oplossing erbij, en bewaard zodat het incidentmanagementproces wordt verbeterd. Er kan lering worden getrokken uit het overzicht met het aantal incidenten en het type incidenten en hier kan vervolgens op worden geacteerd.

2.4 Hoe te gebruiken?

Afhankelijk van de aard van het incident en de grootte van het response team, kan het raadzaam en praktisch zijn om een aantal van de checklist stappen en sub-stappen parallel aan te pakken. Bijvoorbeeld: zodra de oorzaak van een incident wordt bepaald (stap 2),

remediatie van de oorzaak en het herstel van de functie (stap 3) kan worden gestart, terwijl documentatie activiteiten van stap 2.7 worden uitgevoerd (zie bijlage 1 voor een uitgebreide beschrijving van de stappen die gelden bij een major incident of een ernstig security incident).

Het is verstandig om de paraatheid van de Nationale ombudsman op het gebied van 'security incident response' periodiek te oefenen op een manier vergelijkbaar met een noodsituatie planning. Geleerde lessen moeten zo nodig in de checklist, respons procedures, en / of de toewijzing van hulpmiddelen worden opgenomen.

Het stappenplan in bijlage 1 bevat acties die nodig zijn om de meest ernstige veiligheidsincidenten aan te pakken, dat wil zeggen: de blootstelling van persoonlijk identificeerbare informatie beschermd door wetten, standaarden en / of contracten met partijen van buiten de Nationale ombudsman. Het kan ook effectief worden gebruikt om andere veiligheidsincidenten aan te pakken, bijvoorbeeld: het beschadigen van openbare websites, ongeoorloofde toegang tot vertrouwelijke, maar niet wettelijk beschermde gegevens, of het verlies van vertrouwelijke papieren dossiers. In de praktijk zijn de meeste incidenten 'minor incidenten'. Ook deze incidenten moeten geregistreerd en netjes afgehandeld worden. Een op het 'minor incident' proces toesneden stappenplan is opgenomen in bijlage 2.

Gezien de trend naar meer gebruik van derden, met inbegrip van Cloud computing-leveranciers voor het leveren van diensten die gebruik maken van verzamelen, opslaan en/of verwerken van gegevens, dient de Nationale Ombudsman rekening te houden met de gedeelde verantwoordelijkheid voor de incident response. Dit is vaak noodzakelijk door dergelijke overeenkomsten. Deze checklist biedt stappen die moeten gebeuren, ongeacht de locatie van een mogelijke inbreuk op de gegevensbeveiliging. Wie de verantwoordelijkheid moet nemen voor elk van deze stappen als een derde partij betrokken is, zal variëren afhankelijk van de aard van de externe dienst, evenals de beveiliging gerelateerde termen van het contract tussen de Nationale ombudsman en die partij.

3 Aandachtspunten

Welke aspecten komen nog meer bij het incidentmanagementproces kijken? Hieronder staan enkele aspecten die belangrijk zijn voor het incidentmanagementproces.

3.1 Logging

Bij het onderzoek naar mogelijke incidenten wordt veelvuldig gebruik gemaakt van de controle op logging uit systemen, netwerkkapparatuur en programma's. Logbronnen worden gebruikt door een monitoring- en responsdienst die detecteert of er kwetsbaarheden of incidenten hebben plaatsgevonden. Los van de detectie, worden logs ook veelvuldig achteraf gebruikt bij het reconstrueren van een incident of om te ontdekken welke systemen nog meer geraakt zijn. Logs moeten bewaard worden volgens vaste regels en kennen per soort logging een bewaartermijn waarvan afgeweken kan worden (verlenging) als er een vermoeden is van een incident. Als logs op de juiste wijze bewaard en behandeld worden, kunnen logs ook dienen als bewijsmateriaal voor de wet. Let hierbij wel op dat logs persoonsgerelateerde of privacygevoelige informatie kunnen bevatten, en dat logs zodanig bewaard moeten worden dat deze niet zomaar kunnen worden ingezien of worden gewijzigd. Zie hiervoor de 'Aanwijzing Logging' van de IBD. Voor de controle op logging is een voorbeeld cheat sheet te vinden op: <http://www.securitywarriorconsulting.com/security-incident-log-review-checklist.docx>.

3.2 Voorbereiding

Rond incidenten kunnen voorbereidingen getroffen en geoefend worden. Voor incidenten met een mogelijke hoge impact is het wenselijk om dat regelmatig te doen.

In de voorbereiding is het ook belangrijk om iedereen die betrokken zal zijn bij het proces te informeren. Zorg voor overzichten met namen/functies en telefoonlijsten die ook offline beschikbaar zijn. Denk na over communicatie wanneer bijvoorbeeld het totale ICT-infrastructuur (óók VOIP) uitgevallen is of mobiele netwerken overbelast zijn vanwege grote drukte (bij calamiteiten).

3.3 Gouden uur

Het 'gouden uur' is het eerste uur na de ontdekking van het incident. Het is essentieel om het incident in te perken maar ook geen informatie verloren te laten gaan die nodig is voor het onderzoek of het onderzoek achteraf. In het geval van bijvoorbeeld een computerinbraak, het wissen van een schijf en de diefstal van data, kan het nodig zijn om een digitaal forensisch expert in te huren. Deze kan alleen maar onderzoek doen als er zorgvuldig met bewijsmateriaal omgesprongen wordt. De handelingen uitgevoerd in het eerste uur zijn essentieel voor het welslagen van de reactie, maar ook op de bewijsvoering.

3.3.1 Gouden tips

- 1) Vraag bij twijfel advies van een digitaal forensisch expert. Eventueel kan de 24-urshulp van het NCSC worden gebeld.
- 2) Volg uw standaardprocedures.
- 3) Zorg voor volledig inzicht in de juridische consequenties van het incident en uw betrokkenheid. Ga nooit verder dan uw expertise zal toestaan.
- 4) Denk verder dan het apparaat in kwestie en let ook op de papieren documentatie, die in het kantoor ligt en mogelijk ook moet worden beschermd om als mogelijk bewijs te dienen.
- 5) Documenteer nauwkeurig de uitgevoerde acties, deze moeten ook datum en tijd bevatten en gebruik genummerde pagina's.
- 6) Vergeet niet om bij het onderzoek de apparatuur te isoleren vanuit elke netwerkverbinding (Bluetooth, bedraad of draadloos).
- 7) Schakel nooit een gecompromitteerd apparaat aan als het uit staat.
- 8) Als een apparaat is ingeschakeld en het lijkt zo te zijn dat dit actief bezig is met het verwijderen van gegevens of onder externe controle is, dan is het te overwegen het apparaat uit te schakelen door het snoer of de batterij weg te nemen. LET OP: niet uitzetten met de aan/uit knop, dan verdwijnen er mogelijk sporen. Win, indien mogelijk, deskundig advies in alvorens iets te doen.
- 9) Maak desnoods foto's van externe aansluitingen aan het apparaat, zoals printers of USB-drives en van scherm activiteiten die u kunt zien.

4 Incident Prioritering Leidraad

De Incident Prioritering Leidraad beschrijft de regels voor het toekennen van prioriteiten aan incidenten, met inbegrip van de definitie van wat een belangrijk incident is. De incidentprioritering wordt herleid uit een tweetal factoren: urgentie en impact. Het toewijzen van de juiste prioriteit aan een incident is essentieel voor het activeren van de geschikte incidentmaatregelen.

De prioriteit van een incident wordt meestal bepaald door de beoordeling van de impact en urgentie, waarbij:

- Urgentie de maat is voor hoe snel de oplossing van het incident vereist is.
- Impact de maat is voor de omvang van het incident en van de mogelijke schade als gevolg van het incident voordat het kan worden opgelost.

4.1 Incident urgentie

In deze paragraaf worden urgentie categorieën verder uitgewerkt.

Om de urgentie van een incident te bepalen, kiest u altijd uit de hoogste waarde van de desbetreffende categorie:

Categorie Urgentie	Omschrijving
Hoog (H)	▪ De schade veroorzaakt door het incident neemt snel toe. ▪ Werk dat moet worden hersteld door personeel is zeer arbeidsintensief. ▪ Een groot incident kan worden voorkomen door bij een klein incident onmiddellijk te handelen. ▪ Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens
Medium (M)	▪ De schade veroorzaakt door het incident neemt in de tijd aanzienlijk toe. ▪ Er gaat werk verloren, maar dit is relatief snel te herstellen.
Laag (L)	▪ De schade veroorzaakt door het incident neemt in de tijd maar weinig toe. ▪ Het werk dat blijft liggen is niet tijdsintensief.

4.2 Incident impact (categorieën)

In deze paragraaf worden de impact categorieën uitgewerkt, de tabel is slechts een voorbeeld. Om de impact van het incident vast te stellen, kiest u de hoogste desbetreffende categorie:

Categorie Impact	Omschrijving
Hoog (H)	• Relatief veel personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen. Meerdere afdelingen zijn geraakt, het Ombudsplein moet gesloten worden. • Betrokkenen, bijvoorbeeld indieners van klachten en/ of verzoeken zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Gevoelige Persoonsgegevens zijn gecompromitteerd. • De financiële impact van het incident is (naar schatting) hoger dan €10.000,-. • Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Bij de beoordeling van de impact van het datalek zijn van belang: ○ de aard en de omvang van het datalek ○ de aard van de gelekte persoonsgegevens ○ de mate waarin technische beschermingsmaatregelen zijn getroffen ○ de gevolgen voor de persoonlijke levenssfeer van de getroffen personen • Er is reputatieschade, de krant wordt gehaald. • Er zijn lichamelijk gewonden.
Medium (M)	• Enig personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen, bijvoorbeeld een afdeling. • Enkele betrokkenen, bijvoorbeeld indieners van klachten en/ of verzoeken zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn gecompromitteerd. • De financiële impact van het incident is (naar schatting) hoger dan €1.000,- en lager dan €10.000,-. • Er is kans op reputatieschade.
Laag (L)	• Enkele personeelsleden zijn geraakt door het incident en/of kunnen niet meer hun werk doen. • Enkele betrokkenen, bijvoorbeeld indieners van klachten en/ of verzoeken zijn geraakt en/of lijden schade, maar dit is zeer minimaal. Persoonsgegevens zijn gecompromitteerd. • De financiële impact van het incident is (naar schatting) lager dan €1.000,- • Er is geen kans op reputatieschade.

4.3 Incident Prioriteringsklassen

De Incident Prioriteit wordt verkregen door urgentie en impact tegen elkaar af te zetten.

Incident Prioriteiten Matrix

Als er klassen zijn gedefinieerd om urgentie en impact in te schalen, dan kan een Incident Prioriteit Matrix gebruikt worden om prioriteringsklassen te herleiden. In het onderstaande voorbeeld zijn de klassen uitgewerkt met een code en kleuren.

		Impact		
		Hoog	Midden	Laag
Urgentie	Hoog	1	2	3
	Midden	2	3	4
	Laag	3	4	5
Code/kleur	Omschrijving	Reactietijd	Oplossingstijd	
1	Kritiek	Onmiddellijk	1 uur	
2	Hoog	10 minuten	4 uur	
3	Medium	1 uur	8 uur	
4	Laag	4 uur	24 uur	
5	Zeer laag	1 dag	1 week	

4.3.1 Omstandigheden die het noodzakelijk maken dat een incident behandeld wordt als een groot incident

Grote incidenten hebben een ander soort Incident managementteam nodig en maken gebruik van een gescheiden proces dat speciaal is ingericht voor het behandelen van grote incidenten.

4.3.2 Indicatoren

Niettegenstaande de bovenstaande prioritering, is het vaak nodig om aanvullende, gemakkelijk te begrijpen, indicatoren vast te stellen voor het identificeren van grote incidenten (zie ook de toelichting hieronder op het identificeren van grote incidenten ongevallen). Voorbeelden van dergelijke indicatoren zijn:

- 1) Bepaalde (groepen van) bedrijfskritische diensten, toepassingen of onderdelen van de infrastructuur zijn niet beschikbaar en de geschatte tijd voor herstel is onbekend of extreem lang (nader te specificeren diensten, toepassingen of onderdelen van de infrastructuur).
- 2) Bepaalde (groepen van) vitale bedrijfsfuncties (bedrijfskritische processen) worden beïnvloed en de geschatte tijd voor het herstellen van deze processen tot volledige operationele status is onbekend of extreem lang (specificeren bedrijfskritische processen).

4.3.3 Het identificeren van kritische incidenten

Hoewel helpdeskmedewerkers door ervaring vaak een goed idee hebben ontwikkeld over wat een kritisch incident is, blijft het moeilijk om een eenduidige definitie van dit begrip te geven. Daarom is het waarschijnlijk beter om de definitie zo ruim mogelijk te interpreteren.

Een kritisch incident wordt meestal getypeerd door zijn impact, vooral de impact op gebruikers speelt hierbij een belangrijke rol. Enkele voorbeelden:

- Een deel van de datacommunicatie van en naar de Nationale ombudsman ligt plat door een storing in het netwerk.
- Een belangrijke database blijkt corrupt te zijn.
- Meerdere servers worden geïnfecteerd door een 'worm'.
- Persoonsgegevens en vertrouwelijke informatie van burgers worden per ongeluk op een publiek toegankelijk forum geplaatst.

Bedenk ook dat alle rampen zoals onderkend in een continuïteitsplan, kritische incidenten zijn en ook dat kleinere incidenten door een niet afdoende afhandeling, zich tot kritische incidenten kunnen ontwikkelen.

4.3.4 Belangrijkste eigenschappen van kritische incidenten

Enkele belangrijke gevolgen van kritische incidenten zijn:

- een groot aantal gebruikers/klanten kan of enkele belangrijke gebruikers/klanten kunnen mogelijk geen gebruik maken van diensten of systemen;
- een aantal systemen die belangrijk zijn voor de uitvoering van rampenbestrijding en crisisbeheersing valt uit of is niet benaderbaar;
- de kosten (inclusief gevolgschade) voor gebruikers/klanten of voor de Nationale ombudsman zijn aanzienlijk of kunnen aanzienlijk worden;
- het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. De Nationale ombudsman zou reputatieschade kunnen oplopen; en:
- de tijd en moeite die nodig zijn om het incident op te lossen waarschijnlijk groot zijn en, indien afspraken zijn vastgelegd in SLA's, het zeer waarschijnlijk is dat afspraken die zijn vastgelegd in die SLA niet kunnen worden nagekomen.

Een kritisch incident kan ook worden omschreven als een 'major (groot) incident' of een 'incident met hoge prioriteit'.

Bijlage 1: Major & Security incident stappenplan

STAP 1: Identificatie Controleer of een incident daadwerkelijk heeft plaatsgevonden. Deze activiteit omvat normaliter de systeembeheerder en eindgebruiker, maar kan ook het gevolg zijn van proactieve detectie van incidenten door de ICT-beveiliging of het systeembeheer. Indien wordt vastgesteld dat het inderdaad een incident is, dan moeten de betreffende instanties gewaarschuwd worden.				
<i>Soort incident²</i>	<i>Gedaan</i>	<i>Taak</i>	<i>Eigenaar</i>	<i>Notities</i>
Ma, S,		1.1 Onmiddellijk blootstelling of schade beperken: - Voorbeeld: Als een elektronisch apparaat is gecompromitteerd: - o Niet gebruiken (niet inloggen) of wijzigen van het apparaat - o Zet het apparaat niet uit - o Haal de netwerkverbindingen er af, maar NIET de voedingskabel (zet het apparaat op 'vliegtuigstand') 1.2 Registreer de melding als incident - Noteer hoe het incident werd ontdekt en welke acties er tot nu toe genomen zijn. Geef een zo specifiek mogelijk antwoord, inclusief data, tijden, en welke apparaten gecompromitteerd zijn, applicaties, websites, et cetera.	Lijnmanager (Leidinggevende) voor het borgen dat dit proces wordt gevolgd en ICT voor de mogelijke afhandeling.	

² Toelichting op 'soort incident':

- Major incident: Ma
- Security incident: S

Ma, S		1.3 Waarschuw onmiddellijk de incidentmanager en de CISO <i>Handleiding: Voeg namen en telefoonnummers, e-mailadressen toe en zorg dat deze online en offline beschikbaar zijn. .</i>	Automatisch proces binnen Topdesk.	
Ma, S (indien van toepassing)		1.4 Indien er data of elektronische apparatuur gestolen of verloren is, dan ook aangifte laten doen door de gebruiker of eigenaar van het apparaat bij de politie. <i>Handleiding: Deze stap alleen uitvoeren na overleg en op advies van de CISO of ICT- afdeling.</i>	Gebruiker / eigenaar	
Ma, S		1.5 Voer een voorlopige beoordeling uit van het type en de scope van het incident en de omvang van de blootstelling. Als er potentieel gevoelige informatie blootgesteld is dan moet het management geïnformeerd worden en deze moet tijdens het verloop van het incident op de hoogte gehouden worden: <i>Voorbeelden:</i> a) Hoofd Bestuursbureau b) Hoofd C&O (Persvoorlichting) c) NCSC d) Directeur (eindverantwoording) e) Ambtsdrager (via directeur/ MT-lid) - Start met een logboek waarin gedurende het incident alle activiteiten op datum en tijd kunnen worden vastgelegd. - Indien het incident ook het lekken of verlies van persoonsgegevens betreft, leg dit dan nu vast en meld dit bij de Functionaris Gegevensbescherming.	CISO of incidentmanager	

Ma, S (indien van toepassing)		1.6 Indien er sprake is van criminele activiteiten in verband met het incident moet bepaald worden of de politie mogelijk het onderzoek moet overnemen. Als dat gebeurt zal dit het vervolg van dit schema beïnvloeden.	Incidentmanager	
STAP 2: Schade indamming en beoordeling van de blootstelling Wijs een Incident response-teamleider aan en stel een bij het incident passend, 'Incident response team' samen. Dit team is belast met het beperken van verdere schade als gevolg van het incident. Start een grondige beoordeling van de aard en omvang van het incident en stel vast wat de schade is. Stel bewijsmateriaal veilig.				
Ma, S		2.1 Stel het Incidentresponseteam samen <i>Handleiding: Zorg ervoor dat de vertegenwoordiger van de organisatie-eenheid waar het incident zich voordeed, deelneemt en dat deze persoon hoog genoeg in de organisatie zit om de nodige beslissingen te nemen.</i>	Incidentmanager	
Ma, S		2.2 Beoordeling Incidentresponseproces en de verantwoordelijkheden met het Incidentresponseteam • Verstrek ieder teamlid het huidige incidentmanagement stappenplan. • Vindplaats stappenplan: ○ Serruimte en receptie (fysiek) ○ DMS, offline op laptop (digitaal) • Bespreek de communicatiestrategie. ○ Communicatie binnen de organisatie ○ Woordvoerderslijn naar buiten • Bespreek het belang van het goed in een tijdlijn documenteren en het voorkomen van het verloren raken van onderzoeksgegevens.	De manager van het Incident response team/ incidentmanager	

		<i>Handleiding: Aangaande het bespreken van de regels van de communicatie met het team in deze fase, is het vooral belangrijk om de nauwkeurigheid van de feiten te waarborgen tussen teamleden onderling en tussen het team en de juiste ambtenaren.</i> <i>Voorbeelden:</i> <i>a) Teamleden mogen niet praten met anderen buiten het team over het incident totdat er daarvoor toestemming is gegeven door het management of de CISO.</i> <i>b) Alle documentatie die door het team geschreven wordt moet op feiten gebaseerd zijn omdat het mogelijk in een strafrechtelijk onderzoek gebruikt kan worden.</i> <i>c) Er is dagelijks overleg tussen de teamleden.</i> <i>d) Het team moet bijhouden hoeveel tijd er besteed wordt en waaraan.</i>		
Ma, S		2.3 Verzamelen en veiligstellen van bewijsmateriaal <i>Handleiding: Verzamel fysiek en digitaal bewijs die tezamen een duidelijke, gedetailleerde beschrijving geven van hoe het incident heeft kunnen plaatsvinden (bijvoorbeeld: hoe de data gecompromitteerd kon worden).</i> <i>Voorbeelden:</i> <i>a) Images van de harddisk(en)</i> <i>b) Netwerkverkeersgegevens van en naar de gecompromitteerde apparatuur</i> <i>c) Werkplek applicatie logs</i> <i>d) Toegangslogs</i>	Incident team	response

		<i>e) Foto's van de omgeving waar het incident plaatsvindt</i>		
S		2.4 Zorg voor, en onderhoud, al het bewijsmateriaal en houd bij waar het zich bevindt en wie er toegang toe heeft. <i>Handleiding: Maak een inventarisatielijst van alle bewijsmateriaal en houdt bij wie, wanneer, wat gedaan heeft met het bewijsmateriaal.</i> <i>Voorbeelden:</i> <i>a) Beschrijf wat exact het bewijsmateriaal is.</i> <i>b) Leg vast wie erbij moest en waarom.</i> <i>c) Leg vast waar en hoe het bewijsmateriaal opgeslagen is.</i> <i>- Kluis; 2 sleutels gaan bij een incident naar de incidentmanager.</i> <i>d) Als apparatuur verplaatst moet worden zorg dan dat de ontvanger getekend heeft voor ontvangst en dat dit bewijs wordt toegevoegd aan de verzameling. Zorg dat de ontvanger weet welke verantwoordelijkheden er zijn.</i>	Incident response team	
Ma, S (indien van toepassing)		2.5 Neem maatregelen om de scope en de impact van het incident in te perken. <i>Voorbeelden:</i> <i>a) Indien het incident betrekking heeft op gevoelige gegevens die onjuist geplaatst zijn op publiek toegankelijke websites, verwijder dan de actieve en opgeslagen inhoud en verzoek om verwijdering van de</i>	Incident response team	

		<i>gecachte³ of in proxy opgeslagen webpagina('s), die geïndexeerd zijn door zoekmachine bedrijven en andere Internet-archief bedrijven, zoals bijvoorbeeld de Wayback Machine.</i> b) <i>Verander mogelijk gecompromitteerde wachtwoorden.</i> c) <i>Stak de exploitatie van een gecompromitteerde applicatie of server.</i>		
S		2.6 Voer forensisch onderzoek uit – of laat dit uitvoeren – en leg dit vast: 1. Analyseer bewijsmateriaal 2. Voer een reconstructie uit van het incident 3. Zorg voor gedetailleerde documentatie <i>Handleiding: Bewaar origineel bewijsmateriaal en werk alleen op een kopie van de data. Zorg voor minimale verstoring van de bedrijfsvoering, zorg voor herleidbare en herhaalbare resultaten.</i>	Incident response team (indien extern: in overleg met inkoop)	
Ma, S		2.7 Maak de definitieve schatting af, en de documentatie over soort en afbakening van de blootgestelde data, evenals de beschikbaarheid en het soort van contactinformatie van de betrokken personen.	Incident response team	
Ma, S (indien van toepassing)		2.8 Geef mogelijk een voorwaarschuwing aan de Autoriteit Persoonsgegevens. Handleiding: Als er een datalek is en deze valt onder de meldplicht datalekken van de AVG, dan moet er op basis van de beschikbare gegevens	Functionaris Gegevensbescherming	

³ Een cache (spreek uit: kesj of kasj, van het Franse werkwoord 'cacher', verbergen) is een opslagplaats waarin gegevens tijdelijk worden opgeslagen om sneller toegang tot deze data mogelijk te maken. Essentieel van een cache is ook dat het transparant is in die zin dat het bij het ophalen van data niet zichtbaar is of het bij de originele bron wordt opgehaald of uit de cache wordt gehaald, afgezien de korte toegangstijd.

		een voormelding gedaan worden bij de Autoriteit Persoonsgegevens.		
STAP 3: Remediatie en herstel Neem maatregelen om de oorzaak van het incident te blokkeren of te verwijderen, verminder de impact door verdere blootstelling van de gevoelige gegevens te voorkomen, maak een start om de bedrijfsprocessen te herstarten als deze gestopt waren als gevolg van het incident en zorg ervoor dat risico's die verband houden met dit incident worden gemitigeerd.				
Ma, S		3.1 Ga terug naar stap 2.4 en zoek naar aanvullende manieren om de blootstelling te beperken. <i>Voorbeelden:</i> a) Run periodiek web-queries om u er van te verzekeren dat de data niet verder is verspreid of gecached. b) Beoordeel de inventarisatie van getroffen hardware en systemen en wijzig verder waar nodig de wachtwoorden die mogelijk gecorrumpeerd zijn. c) Stop eventueel gecorrumpeerde diensten of applicaties en zorg voor work-arounds	Incident team	response
Ma, S		3.2 Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatie risico's voor gevoelige dataopslag <i>Voorbeelden:</i> a) Run vulnerability scans op getroffen systemen; b) Beoordeel en bepaal waar de data zich bevindt en wijzig dit indien nodig om een hogere beschermingsgraad te verzekeren.	Incident team	response

		c) <i>Beperk de toegang tot systemen tot uitsluitend degenen die toegang nodig hebben.</i> d) <i>Gebruik software tools om gevoelige data te vinden, te verwijderen en te beschermen, bijvoorbeeld: Identity Finder.</i> e) <i>Herstel de getroffen objecten.</i>		
Ma, S		3.3 Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is kunnen ze weer in gebruik genomen worden.	Incident response team	
STAP 4: Kennisgeving Bepaal welke gegevens mogelijk zijn blootgesteld door het incident en stel de getroffen en in kennis van het feit dat hun gegevens blootgesteld zijn. Snelheid is geboden indien er persoonsgegevens verloren zijn gegaan of bekend geworden zijn aan niet rechthebbenden. Informeer indien noodzakelijk andere overheidsinstanties, zoals het NCSC en/of de politie. Bij sommige incidenten is het wettelijk verplicht een melding te doen naar andere instanties. Snelheid is ook belangrijk vanuit een PR-oogpunt. Afhankelijk van de aard van het incident kunnen sommige stappen parallel uitgevoerd worden.				
Ma, S		4.1 Neem beslissingen op basis van de bevindingen van het Incident response team - Leidt het incident tot een beperkte beschikbaarheid van kritische informatiesystemen of tot een inbreuk op integriteit of vertrouwelijkheid van kritische gegevens? En geeft de mate van risico blootstelling de noodzaak tot het informeren van getroffen?⁴ - Zo ja, • Indien van toepassing, is het de taak van rechtshandhaving om de betrokken partijen te informeren?	Incidentmanager	

⁴ Bijvoorbeeld bij niet versleutelde persoonsgegevens die gelekt zijn.

		• Wie gaat het schrijven uitgeven? • Wie zal zich bezighouden met het beantwoorden van telefoon en e-mail op vragen van de betrokken personen? Rechtvaardigt het verwachte volume het opzetten of inzetten van een call center? • Is het noodzakelijk om een officieel persbericht te plaatsen op de website van de Nationale ombudsman? - Als er geen kans is geweest op blootstelling van informatie aan buitenstaanders, dan kan eventueel meteen doorgedaan worden naar stap 4.5.		
Ma, S (Indien van toepassing)		4.2 Indien het een incident betreft met persoonsgegevens waarbij een aanzienlijke kans bestaat op ernstige nadelige gevolgen voor de betrokkene dient de toezichthouder onverwijld in kennis gesteld te worden. Is er sprake van een hoog risico voor betrokkenen dan dienen deze ook in kennis gesteld te worden.⁵ <i>Handleiding:</i> <i>Indien er persoonsgegevens betrokken zijn bij het incident zie dan het datalekken protocol.</i>	Management en Functionaris gegevensbescherming	
Ma, S		4.3 Zet telefoon en e-mail ondersteuning op in geval van vragen: - Stel een team samen. - Zorg voor voldoende infrastructuur, beoordeel of de lijn en e-mail capaciteit voldoende is. - Kies een geschikt telefoonnummer om te gebruiken. - Kies een geschikt e-mailadres om te gebruiken. - Bedenk van te voren de reacties op de verwachte vragen. - Train het team.	Incidentmanager samen met CenO, geadviseerd door de CISO of door het Incident response team	

⁵ Art 33 en 34 van de AVG: Melding van inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene..

Ma, S (Indien van toepassing)		4.4 Als in stap 4.1 een website gekozen is om te communiceren: - Verzin een URL en website locatie. - Voorkom toegang totdat de website live mag gaan. - Bereid de inhoud voor. <i>Handleiding:</i> a) Websites worden vooral gemaakt als het aantal getroffen en te groot is of omdat niet alle mensen bekend zijn. b) De website content moet goedgekeurd worden.	Incidentmanager samen met CenO, geadviseerd door de CISO of door het Incident response team	
Ma, S (Indien van toepassing)		4.5 Voorbereiding schriftelijke informatieverstrekking aan getroffen en: - Bedenk het onderwerp. - Schrijf een concept tekst in de huisstijl. <i>Handleiding:</i> De inhoud van de brief moet zijn goedgekeurd door het management en door voorlichting.	Incidentmanager geadviseerd door de intern klachtenbehandelaar, CenO en de CISO of door het Incident response team	
Ma, S (Indien van toepassing)		4.6 Als er een noodzaak of een verplichting is, informeer de politie en doe aangifte.	Management	
S		4.7 Informeer het NCSC.	CISO na afstemming met het management	

Ma, S (Indien van toepassing)		4.8 Doe de definitieve melding aan de Autoriteit Persoonsgegevens (AP) als er bij Stap 2.8 een voormelding gedaan is. Doe een gemotiveerde melding aan de AP als er bij Stap 2.8 geen voormelding gedaan is en er toch meldplichtige persoonsgegevens gelect zijn. (Gemotiveerd, omdat als bij een AP melding meer dan 72 uur vergaan zijn sinds de ontdekking van het datalek, je moet uitleggen waarom je pas na 72 uur een melding doet.)	Functionaris Gegevensbescherming	
Ma, S (Indien van toepassing)		4.9 Informeer derde partijen zoals service providers als hiermee het risico van identiteitsdiefstal verkleind kan worden of als dat is vastgelegd in het respectievelijke contract.	Afhankelijk van het type leverancier: CenO of Inkoop	
Ma, S (Indien van toepassing)		4.10 Als er bankgegevens blootgesteld zijn aan niet rechthebbenden, informeer dan de bank of creditcard firma's.	Controller	
Ma, S		4.11 Coördineer de gelijktijdige communicatie-acties zodat de verschillende informatiestromen gelijktijdig plaatsvinden.	CenO (Voorlichting)	

2.8 Neem maatregelen om de scope en de impact van het incident in te perken. <i>Voorbeelden:</i> d) Indien het incident betrekking heeft op gevoelige gegevens die onjuist geplaatst zijn op publiek toegankelijke websites, verwijder dan de actieve en opgeslagen inhoud en verzoek om verwijdering van de gecachte of in proxy opgeslagen webpagina('s), die geïndexeerd zijn door zoekmachine bedrijven en andere Internet-archief bedrijven, zoals bijvoorbeeld de Wayback Machine. e) Verander mogelijk gecompromitteerde wachtwoorden. f) Staak de exploitatie van een gecompromitteerde applicatie of server.	Incident response team	
STAP 3: Remediatie en herstel Neem maatregelen om de oorzaak van het incident te blokkeren of te verwijderen, verminder de impact door verdere blootstelling van de gevoelige gegevens te voorkomen, maak een start om de bedrijfsprocessen te herstarten als deze gestopt waren als gevolg van het incident en zorg ervoor dat risico's die verband houden met dit incident worden gemitigeerd.		
3.4 Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatie risico's voor gevoelige dataopslag	Incident response team	
3.5 Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is kunnen ze weer in gebruik genomen worden.	Incident response team	
STAP 4: Kennisgeving Bepaal welke gegevens mogelijk zijn blootgesteld door het incident en stel de getroffen en in kennis van het feit dat hun gegevens blootgesteld zijn. Snelheid is geboden indien er persoonsgegevens verloren zijn gegaan of bekend geworden zijn aan niet rechthebbenden. Informeer indien noodzakelijk andere overheidsinstanties, zoals het NCSC en/of de politie. Bij sommige incidenten is het wettelijk verplicht een melding te doen naar andere instanties. Snelheid is ook belangrijk vanuit een PR-oogpunt. Afhankelijk van de aard van het incident kunnen sommige stappen parallel uitgevoerd worden.		
4.12 (optioneel) Als er een noodzaak of een verplichting is, informeer de politie en doe aangifte.	Management	

Bijlage 3: Checklist Incident response

Stakeholder	Verantwoordelijkheid	Contactgegevens	Indien niet beschikbaar
Incidentmanager	Beheren van het incidentmanagementproces en verantwoordelijk voor de externe communicatie	[redacted] +31 6 [redacted] [redacted]@nationaleombudsman.nl	[redacted] +31 6 [redacted] [redacted]@nationaleombudsman.nl
Systeembeheerder	Verzamelen van technische informatie en incident informatie	[redacted] +31 6 [redacted] +31 7 [redacted] [redacted]@nationaleombudsman.nl	[redacted] +31 6 [redacted] +31 7 [redacted] [redacted]@nationaleombudsman.nl
Helpdesk ICT	Verzamelen van technische informatie en incident informatie	[redacted] +31 6 [redacted] +31 7 [redacted] [redacted]@nationaleombudsman.nl	ICT (dit gaat automatisch: [redacted], [redacted] [redacted] en [redacted])
CISO	Beoordelen en begeleiden van incidenten m.b.t inbreuk op de beschikbaarheid (>2uur) integriteit en vertrouwelijk.	[redacted] +31 6 [redacted] [redacted]@nationaleombudsman.nl	[redacted] +31 6 [redacted] [redacted]@nationaleombudsman.nl
FG	Beoordelen en begeleiden van incidenten die tot een datalek kunnen of hebben geleid.	[redacted] +31 6 [redacted] [redacted]@nationaleombudsman.nl	[redacted] +31 6 [redacted] [redacted]@nationaleombudsman.nl
Cyber Response leverancier	Verantwoordelijk voor het verzamelen en beschermen van bewijsmateriaal. Indien nodig ook voor het geven van advies m.b.t een incident.	Ilionx 088 05 90 500	NCSC 07 [redacted] info@ncsc.nl bij nood: [redacted]@ncsc.nl of 07 [redacted]
Webcare en Social Media	Verantwoordelijk voor communicatie over incidenten	Website No: [redacted] +31 7 [redacted] [redacted]@nationaleombudsman.nl	

	(bereikbaarheid No) naar buitenwereld	Website KOM: [redacted] +31 7 [redacted] [redacted]@dekinderombudsman.nl Socials: [redacted] +31 7 [redacted] [redacted]@nationaleombudsman.nl,	Socials: [redacted] +31 7 [redacted] [redacted]@nationaleombudsman.nl, en [redacted] +31 70 356 36 83 [redacted]@nationaleombudsman.nl
MT-aanspreekpunt	Verantwoordelijk voor de communicatie naar het MT en bevoegd om beslissingen te nemen.	[redacted] +31 6 [redacted] [redacted]@nationaleombudsman.nl	[redacted] +31 6 [redacted] [redacted]@nationaleombudsman.nl
VISMA Circle	Zaaksysteem Verseon	Service Center +31 (0) 46 - 420 93 22 https://circlesoftware.topdesk.net/	n.v.t.
Caesar	Oracle	tel: +31 (0) 88 2404200 info@caesarexperts.nl	n.v.t.
Proact	IT Infra (1 ^e leverancier)	[redacted] (Projectmanager) 06 [redacted] [redacted]@proact.nl	[redacted] (Accountmanager) 06 [redacted] [redacted]@proact.nl [redacted] (Directeur Service Operations) 06 [redacted] [redacted]@proact.nl
[redacted]	IT Infra (2 ^e leverancier)	[redacted] (servicemanager) 06 [redacted] [redacted]@brunel.net	[redacted] (Managing consultant) 06 [redacted] [redacted]@brunel.net
AskRoger	Telefonie	Support & servicedesk 08 [redacted]⁶ [redacted]@askroger.nl	[redacted] (Accountmanager) 08 [redacted] of 06- [redacted]
SWIS	Website No & Website KOM	[redacted] (Teamleider) 07 [redacted] [redacted]@swis.nl	[redacted] (Senior Accountmanager) 06- [redacted] [redacted]@swis.nl

⁶ De No heeft geen 24x7 supportcontract bij AskRoger

Formulier wijzigingsbeheer

A. Beschrijving

Naam wijziging

DMS dossier (= wijzigingsnummer)

Aanvrager van de wijziging

Beoogd resultaat

Samenvatting van de wijziging

Wanneer gaat het in (datum)

Prioriteit (met toelichting)

Indicatie kosten

(Budgethouder / Jaarplan)

B. Impact (inclusief tijd, geld en risico's)

Impact op proces en organisatie?

(geen, laag, midden, hoog, met toelichting)

Proceseigenaar? (naam)

Akkoord ja/nee

Impact op Applicaties?

(geen, laag, midden, hoog, met toelichting en benodigde uren)

Middel (applicatie) eigenaar (naam)

Akkoord ja/nee

Impact op IT infrastructuur?

(geen, laag, midden, hoog, met toelichting en benodigde uren)

Middel (infrastructuur) eigenaar (naam)

akkoord ja/nee

Impact op informatiebeveiliging?

(geen, laag, midden, hoog, met toelichting)

BIA nodig?

Impact op privacy

(geen, laag, midden, hoog, met toelichting)

DPIA nodig?

C. Toestemming wijziging

Advies CAB

Advies CDB (CIO overleg)

Conclusie

Uitvoeren / aanhouden / niet uitvoeren en afsluiten

D. Vrijgave voor productie

Advies CISO (al dan niet na BIA)

Advies FG (al dan niet na DPIA)

Vrijgave advies Functioneel beheerder
na test (*datum en toelichting*)

Vrijgave advies Technisch beheer na
controle (*datum en toelichting*)

Vrijgave advies van de Aanvrager na
gebruikersacceptatietest (*datum en
toelichting*)

Akkoord opdrachtgever tot gebruikname
(*datum*)

Wijzigingsbeheer

PROCES
BESTUURSBUREAU

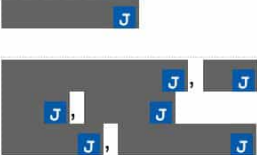
Document classificatie

Vertrouwelijk

Versiebeheer

Versienummer	2.2
Gemaakt door	
Goedgekeurd door	
Datum eerste versie	8 oktober 2020
Laatst bijgewerkt	3 juni 2022

Geschiedenis wijzigingen

Datum	Versie	Aangepast door	Beschrijving van de wijziging
12-10-2020	1.2		Bijlage 2 toegevoegd
20-10-2020	1.3		Impactanalyse in de tekst ingepast
02-11-2020	1.4		
09-11-2020	1.5		BIV-classificatie waardes toegevoegd
02-09-2021	1.6		Proces specifiek gemaakt voor technische wijzigingen en review door CISO
08-09-2021	1.7		Review
20-11-2021	1.9		Verwerking review
15-12-2021	1.9		Review
17-12-2021	1.91		Review
21-12-2021	1.92		Review & aanpassing vormgeving
21-12-2021	1.93		Review en opmerkingen
24-12-2021	1.94		Review en opmerkingen
25-12-2021	1.98		Review en opmerkingen verwerkt.
25-01-2022	2.0		Versie vastgesteld in BVO
23-05-2022	2.1		Aanpassingen n.a.v. evaluatie gebruik
03-06-2022	2.2		Review laatste versie

Inhoudsopgave

1	Inleiding	3
1.1	Doel van wijzigingsbeheer	3
1.2	Definitie van wijziging	3
1.3	Uitzonderingen	3
2	Proces wijzigingsbeheer	5
2.1	Processtappen wijzigingsbeheer	5
2.1.1	Registreren	5
2.1.2	Classificeren	5
2.1.3	Uitvoering wijziging	5
2.1.4	Evalueren	6
2.1.5	Afsluiten wijziging	6
2.2	Procesflow wijzigingsbeheer	7
2.3	Rollen en verantwoordelijkheden	7
3	Belangrijke uitgangspunten	9

1 Inleiding

1.1 Doel van wijzigingsbeheer

Het proces van wijzigingsbeheer heeft als doel ervoor te zorgen dat wijzigingen op de informatievoorziening (ICT-middelen en -diensten) efficiënt en effectief worden doorgevoerd met zo min mogelijk verstoring van de kwaliteit van de dienstverlening, zodat deze dienstverlening blijft voldoen aan de eisen die hieraan zijn gesteld. Om dit te bereiken moeten wijzigingen, vóór deze worden uitgevoerd, worden getoetst op de mogelijke impact die ze kunnen hebben op de informatievoorziening. Naast de toets op de impact dient ook getoetst te worden op de waarschijnlijkheid dat de impact zich voordoet.

Andere processen, zoals bijv. incidentmanagement en patchmanagement, kunnen ertoe leiden dat een wijziging nodig is. Indien dit het geval is dan zal vanuit deze processen het wijzigingsbeheerproces worden opgestart om de wijziging op een gestructureerde manier te laten verlopen.

Wijzigingsbeheer vervult hiermee twee belangrijke functies:

1. Borgen dat wijzigingen aantoonbaar, verantwoord en kosteneffectief worden uitgevoerd.
2. Het adequaat en effectief managen van de mogelijke impact van de wijziging op de bedrijfsvoering. Dit gebeurt onder andere door het implementeren van mitigerende of herstellende maatregelen.

Het proces van wijzigingsbeheer is een verplicht onderdeel uit de BIO. De No heeft om dit document op te stellen gebruik gemaakt van de door de IBD ter beschikking gestelde handreiking Wijzigingsbeheer. Deze handreiking heeft gediend als uitgangspunt en is op onderdelen op de No toegespitst.

1.2 Definitie van wijziging

Een wijziging binnen de context van wijzigingsbeheer is de toevoeging, verandering of verwijdering die een effect kan hebben op de informatievoorziening. De scope is gericht op alle wijzigingen met betrekking tot informatievoorziening en IT-diensten inclusief de daarbij behorende architecturen, processen, instrumenten, meetwaarden en documentatie.

Een wijziging kan voortkomen uit een functionele behoefte of een noodzaak (bijvoorbeeld bij informatiebeveiligingsrisico's en/of incidenten). Als er sprake is van een midden tot hoge impact dan betekent dit dat het niet gaat om een standaard wijziging en dus dat deze procedure gevolgd dient te worden. In het bepalen van de mogelijke impact is een pragmatische kijk en maatvoering belangrijk.

Indien zich een wijziging voordoet dan dient allereerst te worden bepaald om wat voor type wijziging het gaat. Binnen de No worden drie verschillende typen wijzigingen onderkend.

1. Standaard wijzigingen (zoals bijvoorbeeld het aanmaken van een account of mailbox of toekennen van een autorisatie).
2. Niet standaard wijzigingen (Request for change (RFC) of Verzoek tot wijziging (VTW)).
3. Kritieke wijzigingen zoals bijvoorbeeld een (beveiligings)update op een applicatie of informatiesysteem.

Deze procedure is alleen van toepassing op de niet standaard en kritieke wijzigingen.

Vervolgens dient gekeken te worden naar de mogelijke impact die de wijziging kan hebben op de bedrijfsvoering. Dit wordt gedaan op basis van de zogenaamde BIV-aspecten:

Beschikbaarheid: in welke mate kan het doorvoeren van de wijziging impact hebben op de beschikbaarheid van het informatiesysteem.

Integriteit: In welke mate kan het doorvoeren van de wijziging impact hebben op de integriteit van het informatiesysteem.

Vertrouwelijkheid: In welke mate kan het doorvoeren van de wijziging impact hebben op de vertrouwelijkheid van het informatiesysteem.

1.3 Uitzonderingen

Er kunnen zich situaties voordoen waarbij het niet wenselijk of mogelijk is om deze procedure te volgen om de wijziging door te voeren. Indien er sprake is van een situatie waarbij het volgen van deze

procedure ten opzichte van het direct uitvoeren van de wijziging mogelijk zou kunnen leiden tot onacceptabele gevolgen dan kan de CIO in overleg met de CISO en/of FG besluiten dat dit proces geheel of gedeelte niet gevolgd hoeft te worden. Deze situatie zou zich bijvoorbeeld kunnen voordoen indien de No vanuit het NCSC op basis van een high-high alert per direct een wijziging moet uitvoeren en het volgen van het proces zou mogelijk zou kunnen leiden tot onacceptabele tussentijdse risico's.

VERTROUWELIJK

2 Proces wijzigingsbeheer

Het wijzigingsbeheer proces bestaat uit de hierna beschreven stappen.

2.1 Processtappen wijzigingsbeheer

2.1.1 Registreren

Wijzigingsbeheer heeft onder meer als doel dat wijzigingen conform dit beleid worden uitgevoerd en naar behoren geregistreerd worden. Het wijzigingsformulier (onderdeel A) dient gebruikt te worden om wijzigingen te beschrijven. Dit onderdeel wordt aangeleverd door de aanvrager van het verzoek tot wijziging. Verzoeken tot wijziging worden vervolgens geregistreerd in een servicemanagementapplicatie. De wijzigingscoördinator controleert of de registratie compleet is en of de aanvrager gerechtigd is om de wijziging aan te vragen. Hiervoor gelden de volgende uitgangspunten:

- a. Een wijziging op een informatiesysteem kan niet plaatsvinden zonder het akkoord van de middeleigenaar.
- b. Heeft een wijziging gevolgen voor de werking van een proces, dan dient de procesverantwoordelijke hiervan op de hoogte te zijn en is zijn of haar akkoord op de wijziging noodzakelijk.

Stap a. en b. dienen ook om vast te stellen of de wijziging noodzakelijk is. Eventueel kan dit eerst met de CIO en in het BVO besproken worden.

2.1.2 Classificeren

In de processtap classificeren stelt de wijzigingscoördinator vast of er sprake is van een wijziging en deelt de wijzigingscoördinator het verzoek tot wijziging in naar categorie en prioriteit. De wijzigingscoördinator maakt hierbij gebruik van het door de aanvrager ingevulde formulier. Indien nodig wordt ontbrekende informatie over de impact verzameld om te kunnen classificeren.

2.1.3 Uitvoering wijziging

2.1.3.1 Adviseren en besluiten over uitvoering wijziging

Ten aanzien van bepaalde wijzigingen kent de No twee gremia waarin gesproken en besloten kan worden over de uitvoering van wijzigingen waarvan is vastgesteld dat de impact groot is. Dit zijn de Change Advisory Board (CAB) en de Change Decision Board (CDB).

Change Advisory Board (CAB)

De CAB is een overleg waarin gesproken wordt over een of meer wijzigingen die in dezelfde periode plaatsvinden. Het CAB komt bij elkaar wanneer de impact van een of meer van die wijzigingen hoog is. De CAB beoordeelt of alle aspecten van de wijziging in beeld zijn, of de wijziging verantwoord doorgevoerd kan worden en welke mitigerende maatregelen gewenst zijn om risico's te beperken. Ook kijkt de CAB naar de planning en de onderlinge afhankelijkheden van de verschillende wijzigingen. Het CAB komt met een advies voor de CDB. Deelnemers van de CAB zijn:

- Wijzigingscoördinator
- Informatiemanager/ CISO
- Functionaris gegevensbescherming
- Architect en/of
- Adviseur
- Systeemeigenaar (op uitnodiging)
- Aanvrager wijziging (op uitnodiging)

Change Decision Board (CDB)

De CDB besluit over voorgestelde wijzigingen waarvan de impact hoog is. Met name kijkt de CDB of de kosten van de wijziging in verhouding zijn met de baten en of de resterende risico's geaccepteerd kunnen worden. De CDB is geen apart gremium maar is onderdeel van het CIO-overleg. Dit overleg vindt eens in de zes weken plaats. Deelnemers van het CIO-overleg, en daarmee de CDB zijn:

- CIO
- Procesverantwoordelijke uitvoeringsprocessen
- Coördinator i-regie

- Wijzigingscoördinator
- Datamanager
- Informatiemanager/ CISO
- Functionaris Gegevensbescherming
- Architect/ Adviseur
- Archivaris DIV
- Systeemeigenaar (op uitnodiging)
- Aanvrager wijziging (op uitnodiging)

2.1.3.2 Besluiten over uitvoering

Na de classificatie van de wijziging wordt bepaald of de wijziging wordt uitgevoerd en welke prioriteit de uitvoering heeft. In voorkomende gevallen (bijvoorbeeld bij een hoge impact) wordt dit voorgelegd in de CAB voor advies en in de CDB voor besluitvorming. Het wijzigingsformulier vormt hierbij de basis voor besluitvorming. De wijzigingscoördinator is verantwoordelijk voor het inbrengen van een verzoek tot wijziging in de CAB en CDB.

2.1.3.3 Niet uitvoeren verzoek tot wijziging

In het geval dat een wijziging niet in behandeling wordt genomen wordt het verzoek tot wijziging gemotiveerd op 'niet behandelen' gezet en geregistreerd. Deze stap wordt uitgevoerd door de wijzigingscoördinator.

2.1.3.4 Plannen wijziging in release

In deze stap wordt een wijziging ingepland voor uitvoering. Ook het toekennen van benodigde resources voor uitvoering vindt plaats in deze stap. Het inplannen van een wijziging is de verantwoordelijkheid van de wijzigingscoördinator in samenspraak met uitvoerder van de wijziging.

2.1.3.5 Testen

In deze stap wordt de wijziging getest alvorens hij ter accordering wordt aangeboden. De test wordt middels het testproces uitgevoerd en heeft als doel om te verzekeren dat de wijziging geen onvoorziene of onacceptabele gevolgen met zich meebrengt. In bepaalde gevallen, ter beoordeling van de wijzigingscoördinator kan deze stap worden overgeslagen.

2.1.3.6 Accordering

Na het volledig uitvoeren van de wijziging wordt deze voor akkoord voorgelegd aan de CAB en de aanvrager. Dit gebeurt met behulp van onderdeel C uit bijlage 1. Pas na een akkoord op de uitgevoerde wijziging kan doorgedaan worden naar stap 2.1.5. Indien een wijziging niet akkoord wordt bevonden is de wijzigingscoördinator samen met de aanvrager verantwoordelijk voor de aansturing van het herstel van de mogelijke hiaten.

2.1.3.7 Vrijgeven van wijziging

Na akkoord kan de wijziging worden vrijgegeven en daar waar dit van toepassing is kan de wijziging in productie worden genomen.

2.1.4 Evalueren

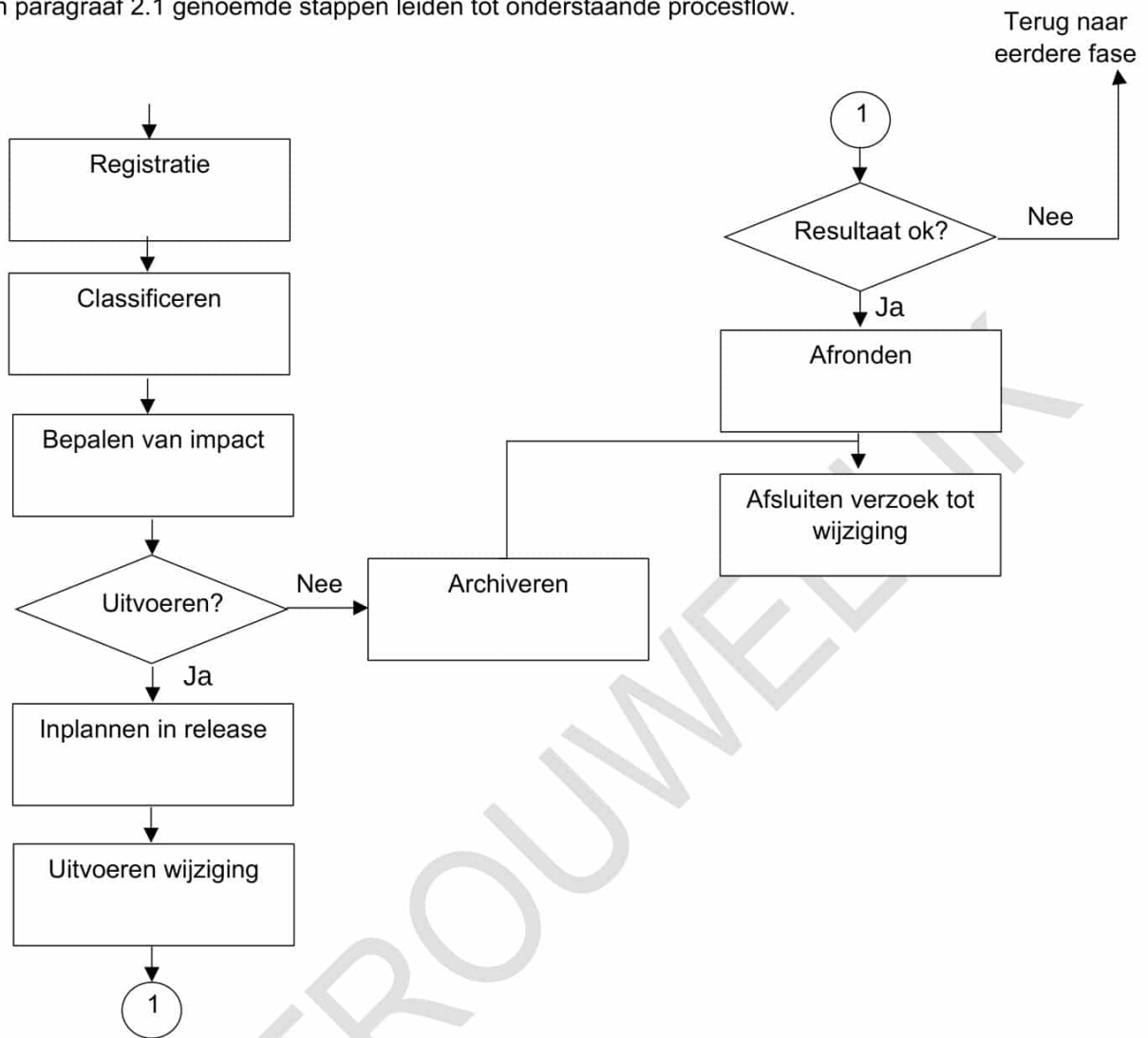
Na de uitvoering van een wijziging vindt een evaluatie plaats met als doel lering te trekken voor opeenvolgende wijzigingen. De wijzigingscoördinator heeft hierbij primair oog voor het volgen van de wijzigingsprocedure. De overige betrokken rollen dienen input te leveren ten aanzien van de door hen uitgevoerde taken.

2.1.5 Afsluiten wijziging

Het verzoek tot wijziging wordt afgesloten in het servicemanagementsysteem door de wijzigingscoördinator. Voor zover dat nog niet heeft plaatsgevonden stelt de wijzigingscoördinator de aanvrager op de hoogte.

2.2 Procesflow wijzigingsbeheer

De in paragraaf 2.1 genoemde stappen leiden tot onderstaande procesflow.



2.3 Rollen en verantwoordelijkheden

De wijzigingscoördinator is primair verantwoordelijk voor het wijzigingsproces. Het maakt hierbij niet uit om wat voor soort wijziging het gaat. Per type wijziging bepaalt de wijzigingscoördinator welke rollen benodigd zijn om de wijziging succesvol uit te voeren.

De volgende actoren hebben bij de meeste wijzigingen een rol en zijn hieronder beschreven.

Wijzigingscoördinator

De wijzigingscoördinator:

- Controleert de volledigheid en juistheid van de registratie van de wijziging inclusief het wijzigingsvoorstel op basis van een door de wijzigingscoördinator opgestelde checklist;
- Ziet erop toe dat de wijzigingsprocedures worden gehandhaafd, en bewaakt de voortgang van de afhandeling van wijzigingen;
- Classificeert in overleg met de aanvrager het wijzigingsvoorstel op basis van prioriteit en categorie;
- Laat op een geaccepteerd wijzigingsvoorstel een impactanalyse uitvoeren, en stelt op basis van de impactanalyse een rapportage op die het volgende bevat:

- Aannames
 - Beperkingen
 - Omvang
 - Consequenties wijzigingsvoorstel
 - Oplossingsalternatief en betrokken configuratie-items
 - Uit te voeren activiteiten
 - Begroting
 - Risicoanalyse met ondersteuning van de CISO
 - DPIA met ondersteuning van de FG.
- Is voorzitter van de CAB, waarin alle expertise is verzameld zodat de wijzigingsvoorstellen op alle aspecten beoordeeld kunnen worden en waarvan de leden samenkomen in het wijzigingsoverleg;
 - Verstrekt aan de CAB de rapportage van de uitgevoerde impactanalyse en de (op basis van de uitgevoerde impactanalyse) gewijzigde uitgifteplanning, en;
 - Neemt deel aan de CDB waarin wordt besloten over de wijziging.

Helpdesk ICT (bij ICT-gerelateerde wijzigingen)

De helpdesk is het startpunt m.b.t wijziging en is verantwoordelijk voor de registratie hiervan in de servicemanagementapplicatie.

Informatiemanager

Idealiter komt een verzoek tot wijziging tot stand in samenspraak met de informatiemanager. De informatiemanager heeft als rol om de informatiebehoefte op te halen bij de gebruikers en dit te vertalen in wijzigingen in het geval van bestaande informatiesystemen of de inkoop/ aanbesteding van nieuwe informatiesystemen.

Middeleigenaar

De middeleigenaar is verantwoordelijk voor de goede werking van het informatiesysteem waarvan hij of zij de eigenaar is en bepaalt of wijzigingen in het informatiesysteem aangebracht mogen worden.

CISO

De CISO is deels ondersteunend in het wijzigingsproces. Dit is bijvoorbeeld het geval indien er een BIA of risicoanalyse uitgevoerd moet worden. Daarnaast toetst de CISO of de impact van bepaalde wijzigingen acceptabel zijn in relatie tot de 'Risicobereidheid'¹ van de organisatie.

FG

De FG is deels ondersteunend in het wijzigingsproces dit is bijvoorbeeld het geval indien er een DPIA uitgevoerd moet worden. Daarnaast toetst de FG of de impact van bepaalde wijzigingen acceptabel zijn in relatie tot privacy vereisten die van toepassing zijn op de organisatie.

NB: Het is de verantwoordelijkheid van de wijzigingscoördinator om de CISO en/of FG te informeren en aan te haken indien dit noodzakelijk is.

Architect

De architect heeft de verantwoordelijkheid om de impact van de wijziging te beoordelen op de bestaande architectuur en deze te toetsen aan de 'Enterprise Principles' van de No.

Functioneel beheer

Functioneel beheer zal in het wijzigingsproces in veel gevallen verantwoordelijk zijn voor de uitvoering, het testen en rapporteren van bevindingen.

¹ De mate van risico, op een breed niveau, die de organisatie bereid is om te accepteren in het streven naar het behalen van de organisatiedoelen. De risicobereidheid bepaalt de allocatie van middelen en helpt de organisatie in het richten van de organisatie, mensen en processen op het ontwerpen van de infrastructuur die nodig is om effectief op risico's te reageren en deze te monitoren.

3 Belangrijke uitgangspunten

- I. De wijzigingscoördinator geeft aan of de wijzigingsprocedure geheel of gedeeltelijk gevolgd moet worden. De opdrachtgever vult daartoe de eerste pagina van het wijzigingsformulier zoveel mogelijk in. Als er impact is op privacy en informatiebeveiliging (beschikbaarheid, integriteit en betrouwbaarheid van de informatieverwerking) zal de wijzigingsprocedure gevolgd moeten worden. Hiervoor kan het nodig zijn dat er een BIA/ Risicoanalyse of DPIA wordt uitgevoerd.
- II. In het formulier wordt beschreven wat de bedoeling is van de wijziging en wat de gevolgen zijn (gebruik hiervoor, indien aanwezig, het beslisdocument van het MT of het BVO). De wijzigingsprocedure is voor de wijzigingscoördinator de checklist voor het communiceren, afstemmen en goedkeuren van de wijziging.
- III. In de functionele specificatie van een wijziging wordt ook aangegeven welke eisen er zijn ten aanzien van de werkprocessen, bedrijfsvoering- en ondersteuning, de applicaties, de technische infrastructuur, informatiebeveiliging en gegevensbescherming en hoe daaraan wordt voldaan.
- IV. De impactbeoordeling informatiebeveiliging (zie formulier Business Impact Analyse) wordt alleen ingevuld bij nieuwe ontwikkelingen of wanneer nog niet eerder een impactbeoordeling is ingevuld. Een bestaande impactbeoordeling kan geactualiseerd worden.
- V. Alle wijzigingen worden door de wijzigingscoördinator gedocumenteerd en periodiek gerapporteerd aan het CIO overleg. Relevante stukken, zoals ook adviezen en instemmingen per email, worden als bijlagen bij het wijzigingsformulier bewaard. Het gaat hierbij alleen om de niet-standaard wijzigingen, ten aanzien van de spoed security patches worden deze in de servicemanagementapplicatie geregistreerd en informeert de servicedesk de wijzigingscoördinator hierover.
- VI. De CISO ziet erop toe dat het wijzigingsbeheer voldoet aan de eisen van de BIO.
- VII. De verantwoordelijke beslist of een wijziging gereed is en doorgevoerd kan worden:
 - a. De procesverantwoordelijke als er impact is op werkprocessen en organisatie.
 - b. De middeleigenaar als er geen impact is op processen en organisatie.
 - c. Het hoofd IT als er geen impact is op processen en organisatie en op applicaties.



BELEID BESCHERMING PERSOONSGEGEVENS

Inhoud

Voorwoord.....	4
Inleiding	4
1. Wat valt er onder privacybeleid?.....	4
1.1 Persoonsgegevens	5
1.2 Verwerkingen van persoonsgegevens.....	5
1.3 Relatie integrale beveiliging, informatiebeveiliging, privacybeleid	5
2. Wie zijn de hoofdpersonen?	6
2.1 Betrokkenen.....	6
2.2 Verwerkingsverantwoordelijke	6
2.3 Verwerker en intern beheerder	6
2.4 Functionaris Gegevensbescherming	7
2.5 Contactpersoon AVG.....	7
2.6 Burgers en bezoekers	7
2.7 Security Officer	8
3. Uitgangspunten privacybeleid Nationale ombudsman	8
3.1 Rechtmatigheid, behoorlijkheid en transparantie.....	8
3.2 Doelbinding	10
3.3 Dataminimalisatie.....	10
3.4 Juistheid	10
3.5 Opslagbeperking	11
3.6 Integriteit en vertrouwelijkheid.....	11
3.7 Verantwoordingsplicht/Accountability	11
4. Organisatorische en technische maatregelen privacybeleid	12
4.1 Aanstelling FG	12
4.2 Contactpersoon AVG per dienst.....	12
4.3 AVG-register	12
4.4 AVG-loket.....	12
4.5 Procedure datalekken	12
4.6 Verwerkersovereenkomsten via Bestuursbureau (Inkoop)	13
4.7 Privacy Impact Assessment	13
4.8 Interne/externe scholing.....	13
4.9 Interne en externe communicatie	13
Bijlage: verklaring van begrippen	14

Voorwoord

De Nationale ombudsman verwerkt in het kader van het primair proces en zijn bedrijfsvoering persoonsgegevens en vindt het belangrijk dat met deze persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk worden behandeld.

De Algemene Verordening Gegevensbescherming (hierna: AVG) biedt waarborgen voor de bescherming van de persoonlijke levenssfeer van natuurlijke personen met betrekking tot het verwerken van persoonsgegevens. De Nationale ombudsman heeft in lijn met het bepaalde in de AVG beleid opgesteld voor het gebruik van persoonsgegevens.

Het privacybeleid heeft tot doel:

- Regels te stellen voor het verwerken van persoonsgegevens door de Nationale ombudsman.
- Informatie te verschaffen aan personen van wie persoonsgegevens door de Nationale ombudsman verwerkt (zullen) worden.
- Bij te dragen aan de transparantie van de regels die door de Nationale ombudsman worden toegepast bij het verwerken van persoonsgegevens.

Het privacybeleid van de Nationale ombudsman valt onder de verantwoordelijkheid van de directeur van de Nationale ombudsman en wordt door het corporate overleg van de No vastgesteld. Het corporate overleg zorgt dat alle medewerkers op de hoogte zijn van dit privacybeleid en het kunnen toepassen op hun dagelijks werkzaamheden. De ambtsdragers van de Nationale ombudsman worden door de directeur op de hoogte gebracht van dit privacybeleid.

Ook relevante externe partijen, zoals burgers, bezoekers en leveranciers, worden van het privacybeleid van de Nationale ombudsman op de hoogte gebracht, bijvoorbeeld door korte verklaringen op internet en in overeenkomsten.

In deze notitie wordt uiteengezet wat het privacybeleid van de Nationale ombudsman inhoudt en hoe dit door alle medewerkers van de ombudsman zal worden nageleefd. Zodat betrokkenen er van op aan kunnen dat met persoonsgegevens veilig en verantwoord wordt omgegaan door de Nationale ombudsman.

Wanneer wordt gesproken over Nationale ombudsman wordt hier bedoeld de ambtelijke organisatie van de Nationale ombudsman.

Inleiding

Privacy is een grondrecht dat is verankerd in de Grondwet, verdragen en in wet- en regelgeving, zoals de AVG. Het recht op privacy is geen absoluut recht maar moet worden afgewogen tegen andere rechten, plichten en belangen. De Nationale ombudsman wil (naast het voldoen aan alle wet- en regelgeving) zorgvuldig, veilig en rechtmatig omgaan met persoonsgegevens, waarbij de belangen van betrokkenen centraal staan. Uitgangspunt is steeds dat er een weging moet plaatsvinden tussen de noodzaak voor het verwerken van persoonsgegevens en de gevolgen van deze verwerking voor het individu.

In een bijlage bij deze notitie wordt een aantal in deze notitie gebruikte begrippen nader toegelicht.

1. Wat valt er onder privacybeleid?

Onder het privacybeleid van de Nationale ombudsman vallen alle verwerkingen van persoonsgegevens. Hieronder worden deze begrippen toegelicht.

1.1 Persoonsgegevens

Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn.

Er zijn vele soorten persoonsgegevens, zoals iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. En aan een foto is iemand ook te herkennen. Een foto is dus net zo goed een persoonsgegeven. En het houdt niet op bij zulke feitelijke gegevens: gegevens die een waardering over een bepaalde persoon inhouden, bijvoorbeeld een beoordeling van een manager, kan ook een persoonsgegeven zijn.

Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden in de wet bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd en mogen niet zomaar verwerkt worden.

Waar in deze notitie over privacy wordt gesproken wordt bedoeld informationele privacy. Dat wil zeggen dat het gaat om het verwerken en verzamelen van persoonlijke data, zoals financiële gegevens, medische gegevens, contactgegevens etc.

1.2 Verwerkingen van persoonsgegevens

Verwerken van persoonsgegevens is een ruim begrip. Het is belangrijk te beseffen dat verwerken gaat over alle handelingen die kunnen worden uitgevoerd met persoonsgegevens: van raadplegen, verzamelen tot en met vernietigen.

De medewerkers van de Nationale ombudsman ondersteunt de Nationale ombudsman bij zijn taken en maakt het werk van de Nationale ombudsman toegankelijk en inzichtelijk voor de samenleving.

Medewerkers van de Nationale ombudsman zorgen onder meer voor klachtbehandeling, onderzoek, verslaglegging, informatievoorziening, documentatie, archivering, beheer van het gebouw, doelmatig en rechtmatig financieel beheer, personeelszaken en externe voorlichting. Om dit werk te kunnen doen is het vaak noodzakelijk persoonsgegevens te verwerken van medewerkers, burgers en bezoekers. Denk bijvoorbeeld aan persoonsgegevens die gebruikt worden voor de toegangspas, de uitvoering van het personeelsbeleid, facturen en declaraties van medewerkers en uitgifte van IT-middelen.

1.3 Relatie integrale beveiliging, informatiebeveiliging, privacybeleid

Integrale beveiliging is de overkoepelende aanpak van beveiliging en bevat onder andere fysieke beveiliging, informatiebeveiliging en privacybeleid. Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken. Daarvoor worden organisatorische, technische en personele maatregelen genomen. De Nationale ombudsman heeft beleid opgesteld voor informatiebeveiliging. Dit beleid is te vinden op het intranet van de Nationale ombudsman.

Bij informatiebeveiliging spelen drie begrippen een sleutelrol, namelijk:

- Beschikbaarheid bevat de garanties dat informatie voor gebruikers beschikbaar is op het moment waarop zij de informatie nodig hebben. Kenmerken van beschikbaarheid zijn tijdigheid, continuïteit en robuustheid.

- Integriteit geeft de mate aan waarin de informatie actueel en correct is. Kenmerken zijn juistheid, volledigheid en geautoriseerdheid van de transacties.
- Vertrouwelijkheid of exclusiviteit is het kwaliteitsbegrip waaronder privacybescherming maar ook de exclusiviteit van informatie gevangen kan worden. Het waarborgt dat alleen geautoriseerden toegang krijgen en dat informatie niet kan uitlekken.

Privacybeleid en informatiebeveiliging zijn niet los van elkaar te zien, maar overlappen elkaar ook niet volledig. Privacybeleid stelt namelijk naast de vraag of de persoonsgegevens goed beveiligd zijn (zie bovenstaande sleutelbegrippen beschikbaarheid, integriteit en vertrouwelijkheid) ook nog aanvullende vragen. Namelijk of de gegevens wel mogen worden verzameld en verder verwerkt, op welke manier, en in hoeverre dit noodzakelijk is. Deze vragen maken geen deel uit van het informatiebeveiligingsbeleid. Daarnaast houdt het privacybeleid zich enkel bezig met persoonsgegevens en gaat informatiebeveiliging over veel meer vormen van informatie.

2. Wie zijn de hoofdpersonen?

De hoofdpersonen van de AVG zijn de betrokkenen, de verwerkersverantwoordelijke en de verwerker. Betrokkenen zijn de personen van wie gegevens worden verwerkt. De verwerkingsverantwoordelijke is degene die doel en middelen vaststelt voor de verwerkingen. En de verwerker is degene die persoonsgegevens verwerkt, maar niet onder het rechtstreeks gezag van de verwerkingsverantwoordelijke staat. Daarnaast zijn er voor de naleving van de AVG binnen de Nationale ombudsman nog een aantal taken/rollen belegd, zoals de Functionaris Gegevensbescherming (FG) en de contactpersonen AVG. Hieronder worden de rollen en functies van deze hoofdpersonen nader toegelicht.

2.1 Betrokkenen

Betrokkenen zijn de personen van wie gegevens worden verwerkt. Voor de Nationale ombudsman kunnen dit de volgende categorieën betrokkenen zijn: ambtsdragers, medewerkers, burgers en bezoekers. Voor elke verwerking van persoonsgegevens moet duidelijk zijn wat de rechten en plichten van elk van deze categorieën zijn. In paragraaf AVG-loket wordt nader ingegaan op de rechten van betrokkenen.

2.2 Verwerkingsverantwoordelijke

De Verwerkingsverantwoordelijke is degene die doel en middelen vaststelt voor de verwerkingen van persoonsgegevens. Voor de organisatie van de Nationale ombudsman is dat de directeur. In de praktijk betekent dit dat elk hoofd van een organisatieonderdeel namens de directeur van de Nationale ombudsman verantwoordelijk is voor alle verwerkingen van persoonsgegevens die binnen het eigen onderdeel plaatsvinden. Wanneer meerdere onderdelen verantwoordelijk zijn voor een verwerking, worden onderling duidelijke afspraken gemaakt wat de respectievelijke verantwoordelijkheden ten aanzien van de AVG zijn en wie als contactpunt voor betrokkenen zal fungeren. Deze afspraken worden opgenomen in het AVG-register.

2.3 Verwerker en intern beheerder

Een verwerker verwerkt persoonsgegevens zonder onder het rechtstreekse gezag van de verwerkingsverantwoordelijke te vallen (iemand of een organisatie buiten de organisatie van de Nationale ombudsman). De verwerker voert slechts een taak uit die de verwerkingsverantwoordelijke heeft uitbesteed.

Wordt de taak uitgevoerd door iemand die wel valt onder rechtstreeks gezag van de verantwoordelijke dan is hij geen verwerker, maar is er sprake van intern beheer. Voordat er persoonsgegevens gedeeld worden met een verwerker moet er een verwerkersovereenkomst worden afgesloten. Dit wordt nader toegelicht in paragraaf 4.6 van deze notitie.

2.4 Functionaris Gegevensbescherming

De Nationale ombudsman heeft sinds ... een functionaris gegevensbescherming (FG) aangesteld. De contactgegevens van de FG zijn te vinden op het intranet en de website van de Nationale ombudsman. De FG heeft als intern toezichthouder een onafhankelijke positie en beschikt over toereikende kennis, voldoende middelen en capaciteit om zijn taken in het kader van de AVG naar behoren te kunnen uitvoeren. Onder deze taken vallen:

- a. Informeren en adviseren van MT en leidinggevenden over hun verplichtingen uit hoofde van wet- en regelgeving in het kader van privacy.
- b. Toezien op de naleving van de relevante wetgeving, het privacybeleid en op de inrichting van de interne privacy organisatie.
- c. Advies leveren bij een Privacy Impact Assessment (PIA), zowel de inhoudelijke beoordeling als de naleving van de voorgenomen beheermaatregelen.
- d. Samenwerken met de centrale toezichthouder, de Autoriteit Persoonsgegevens, in het geval van een onderzoek.
- e. Aanspreekpunt voor betrokkenen (medewerkers en burgers) voor alle aangelegenheden bij de verwerking van hun persoonsgegevens.
- f. Het afleggen van verantwoording over de verwerkingen van persoonsgegevens in het financieel jaarverslag van de Nationale ombudsman.
- g. In geval van incidenten zal de FG (in overleg met de security officer en andere intern betrokkenen) beoordelen of er sprake is van een datalek. Dit wordt zo nodig gemeld bij de Verwerkingsverantwoordelijke en bij de Autoriteit Persoonsgegevens (AP).
- h. Opbouwen en onderhouden van nationaal netwerk.

2.5 Contactpersoon AVG

Binnen elke dienst (organisatieonderdeel) wordt minimaal één contactpersoon AVG benoemd, die over voldoende kennis over de AVG beschikt. De contactpersonen AVG zullen hiervoor regelmatig (interne) scholingsactiviteiten krijgen aangeboden. Deze AVG contactpersoon heeft tenminste de volgende taken:

- a. Fungeren als 'adviesloket' bij vragen binnen de eigen dienst over de AVG.
- b. Inventariseren, beoordelen, bijhouden en melden van verwerkingen persoonsgegevens.
- c. Aanspreekpunt voor de FG bij incidenten (waaronder datalekken) en privacy verzoeken.
- d. Zorgen dat de AVG blijvend onder de aandacht is van de medewerkers van de eigen dienst en draagt zo bij aan het privacy bewustzijn van de medewerkers van de Nationale ombudsman.

2.6 Burgers en bezoekers

De Nationale ombudsman ontvangt dagelijks bezoekers op de website en fysiek in het gebouw van de Nationale ombudsman. Bezoekers van de website en het gebouw van de Nationale ombudsman worden (via een disclaimer en privacy statement) geïnformeerd dat op een veilige en rechtmatige wijze met hun persoonsgegevens wordt omgegaan en worden gewezen op de rechten die zij hebben conform de AVG. In paragraaf 4.9 van deze notitie wordt dit nader toegelicht.

De Nationale ombudsman ontvangt vrijwel dagelijks brieven van derden, die doorgaans binnenkomen bij de Facilitaire Dienst. Dit zijn zowel brieven van burgers als van organisaties, die aandacht vragen voor een veelheid van onderwerpen. Omdat in deze brieven ook persoonsgegevens staan vermeld, worden burgers en organisaties in de ontvangstbevestiging tevens geïnformeerd dat zij bezwaar kunnen maken tegen opname in het uitsluitend intern toegankelijke systeem voor de behandeling van ontvangen brieven. Alle medewerkers hebben toegang tot dit systeem.

2.7 Security Officer

In paragraaf 1.3 van deze notitie is de relatie tussen Privacybeleid en Informatiebeveiligingsbeleid in beeld gebracht.

De security officer is verantwoordelijk voor en coördineert het Informatiebeveiligingsbeleid van de Nationale ombudsman. Vanwege de raakvlakken en overlap zal er regelmatig overleg plaatsvinden tussen de security officer en FG, bijvoorbeeld wanneer er sprake is van incidenten, zoals datalekken of de invoering van nieuwe (technische) maatregelen. Ook met betrekking tot voorlichting, bewustwording en borging van zowel het informatiebeveiligingsbeleid als het privacybeleid zal waar mogelijk samen opgetrokken worden.

3. Uitgangspunten privacybeleid Nationale ombudsman

In de AVG zijn deels open normen opgenomen die een nadere vertaling naar het beleid behoeven. Want wat dient te worden verstaan onder ‘passende’ maatregelen, en ‘niet meer persoonsgegevens gebruiken dan noodzakelijk’. Het privacybeleid biedt hierbij de helpende hand. Het vormt als het ware een baseline die het voor de medewerkers inzichtelijk maakt waar elke ambtelijke dienst minimaal aan moet voldoen. Het kan gebruikt worden als normenkader om de AVG te implementeren en handhaven binnen de verschillende onderdelen. Daarnaast kan een baseline door het MT van de Nationale ombudsman gebruikt worden als sturingsmiddel om het privacybeleid binnen de Nationale ombudsman vorm te geven.

Let op: Deze privacy baseline is nadrukkelijk niet gelijk aan het voldoen aan alle privacy- en gegevensbeschermingseisen die de AVG stelt. Het is geen afvinklijstje van noodzakelijke maatregelen. Voor de Nationale ombudsman blijft het uitgangspunt dat er steeds een weging moet plaatsvinden tussen de noodzaak voor het verwerken van persoonsgegevens en de gevolgen van deze verwerking voor het individu.

Volgens de AVG moeten verwerkingen van persoonsgegevens voldoen aan een aantal beginselen. Deze beginselen vormen het fundament voor het privacybeleid van de Nationale ombudsman, zodat alle verwerkingen rechtmatig, veilig en verantwoord plaatsvinden, en worden hieronder toegelicht.

3.1 Rechtmatigheid, behoorlijkheid en transparantie

Deze drie belangrijke begrippen worden hieronder nader toegelicht.

Rechtmatigheid

Dat wil zeggen dat elke verwerking van persoonsgegevens gebaseerd moet zijn op één van de zes grondslagen die de AVG noemt. Deze lijst is limitatief, dat wil zeggen dat er geen andere gronden kunnen worden aangevoerd. De grondslagen zijn:

- a. Betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden. Let op: deze toestemming moet vrij, specifiek, geïnformeerd en ondubbelzinnig gegeven zijn.
 - ⇒ Deze grondslag bij voorkeur alleen gebruiken als het niet anders kan, zeker in geval er sprake is van een machtsverhouding (werkgever-werknemer, overheid-burger).
- b. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is.
 - ⇒ Denk bijvoorbeeld aan uitvoering van een arbeidsovereenkomst of een bruikleenovereenkomst.
- c. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
 - ⇒ Denk bijvoorbeeld aan de Archiefwet, fiscale bewaarplicht en de Grondwet.
- d. De verwerking is noodzakelijk om de vitale belangen van de betrokkene te beschermen. Deze grondslag zal niet vaak gebruikt worden.
 - ⇒ Het gaat hierbij om levensbedreigende situaties. Is een persoon buiten bewustzijn en is medische hulp geboden? Dan kunnen zonder toestemming direct de noodzakelijke persoonsgegevens verwerkt worden om hulp te bieden.
- e. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
 - ⇒ Het gaat hierbij om relevante taken die in de wet zijn vastgelegd en die nodig zijn om een publieke taak goed te kunnen vervullen. Denk bijvoorbeeld aan de wettelijke taken die de Nationale ombudsman heeft, zoals de behandeling van verzoekschriften. Daarnaast heeft de Nationale ombudsman ook publieke taken, zoals de media informeren over de werkwijze van en de activiteiten van de Nationale ombudsman.
- f. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke. Dat is zo wanneer een verwerking aantoonbaar noodzakelijk is om bedrijfsactiviteiten te verrichten. Bijvoorbeeld het voeren van een personeelsadministratie.
 - ⇒ Denk hierbij bijvoorbeeld aan het belang om het gebouw te beveiligen, het doorsturen van personeelsgegevens tussen diensten of het verwerken van gegevens (inlognamen/wachtwoorden) ten behoeve van netwerkbeveiliging.

Let op:

De grondslagen die hierboven worden genoemd onder b t/m f zorgen ervoor dat het noodzakelijk is dat persoonsgegevens verwerkt worden. Zij zorgen ervoor dat die verwerking aantoonbaar is. De verwerking moet echter behalve aantoonbaar noodzakelijk ook nog proportioneel zijn en voldoen aan de subsidiariteitseis. Dat wil zeggen dat er ook nog nagegaan wordt of de noodzaak om de persoonsgegevens te verwerken in verhouding staat tot de mate van inbreuk in de privacy van de betrokkene. En dat de gekozen verwerking de beste manier is om het doel te bereiken. Wellicht is er een andere, minder ingrijpende manier, of kan worden volstaan met de verwerking van minder persoonsgegevens. Zie in dit kader ook beginsel 3: dataminimalisatie.

Behoorlijkheid

Dat wil zeggen dat de verwerking van persoonsgegevens netjes en verantwoord is, ook wel genoemd 'maatschappelijk betamelijk'.

Transparantie

Dat wil zeggen dat de betrokkene op de hoogte wordt gesteld van het feit dat er verwerking van zijn persoonsgegevens plaatsvindt, en wat de doeleinden van deze verwerking zijn, in heldere en begrijpbare taal. Bovendien moet de betrokkene geïnformeerd worden over zijn rechten en hoe hiervan gebruik kan worden gemaakt. De rechten van betrokken worden nader toegelicht in paragraaf 4.4 van deze notitie.

3.2 Doelbinding

Doelbinding, dat wil zeggen dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens alleen op met dat doel verenigbare wijze worden verwerkt.

Het doel bepaalt welk gebruik van de persoonsgegevens is toegestaan en welk gebruik niet. Zo mogen bijvoorbeeld niet méér persoonsgegevens verzameld en gebruikt worden dan nodig is voor het doel en mogen persoonsgegevens niet langer bewaard worden dan nodig is voor het doel. Het doel beperkt ook de mogelijkheid om eenmaal voor een bepaald doel verzamelde persoonsgegevens, voor een ander doel te gebruiken, tenzij het een verenigbaar doel is.

Denk bijvoorbeeld aan de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden En het bewaren van persoonsgegevens van afgewezen kandidaten na afronding van een sollicitatieprocedure, Of het bewaren van genodigdenlijsten na afloop van een bijeenkomst.

3.3 Dataminimalisatie

Dataminimalisatie, dat wil zeggen dat niet meer persoonsgegevens worden verwerkt dan nodig is voor het doel waarvoor ze verzameld worden. Bij het ontwikkelen van nieuwe diensten en producten wordt nagedacht over welke persoonsgegevens nodig zijn om de dienst te kunnen leveren. Maar ook in bestaande processen moet aandacht zijn voor dataminimalisatie.

Denk bijvoorbeeld aan verdere verwerking van persoonsgegevens voor statistische doeleinden. Hierbij worden persoonsgegevens waar mogelijk geanonimiseerd. Zodat de gegevens wel bewaard kunnen blijven voor statistische doeleinden zonder dat ze tot een individueel persoon herleidbaar zijn. De optimale situatie is alleen de strikt noodzakelijke gegevens verzamelen. Als dat niet lukt kies dan voor de optie om alle andere gegevens direct te verwijderen als blijkt dat deze gegevens overbodig zijn.

Denk bijvoorbeeld aan webformulieren. Om te zorgen dat er niet meer gegevens worden verzameld dan noodzakelijk moeten alleen die persoonsgegevens worden gevraagd die nodig zijn voor het leveren van een dienst. Dataminimalisatie moet bij de standaardinstelling van systemen die gebruikt worden en bij het ontwerp van nieuwe systemen meegenomen worden.

3.4 Juistheid

Juistheid, dat wil zeggen dat de persoonsgegevens die verwerkt worden correct zijn en correct blijven. Maar ook het regelmatig controleren van toegang tot systemen en het actueel houden van verleende machtigingen, vallen onder het beginsel juistheid.

Dit betekent dat alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren. Zie verder het recht op rectificatie van betrokkenen in paragraaf 4.4.

3.5 Opslagbeperking

Opslagbeperking (oftewel bewaartermijnen), dat wil zeggen dat een persoonsgegeven alleen mag worden bewaard als identificeerbaar gegeven, voor zolang als het nodig is voor de doeleinden waarvoor het verzameld is.

Het is wel mogelijk om, als de gegevens geanonimiseerd kunnen worden en daarmee dus niet meer direct of indirect identificatie van een persoon mogelijk maken, de gegevens langer te bewaren. Ook hier gelden trouwens weer de uitzonderingen voor archivering, algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Voor sommige gegevens geldt dat deze gedurende een bepaalde periode niet vernietigd mogen worden. Ze moeten worden bewaard in het archief. Verschillende wetten kennen bepalingen waarin een termijn wordt gesteld gedurende welke de persoonsgegevens, na verwijdering uit de actieve administratie, bewaard moeten blijven. Op het intranet van de Nationale ombudsman zijn de regels omtrent archiveren te vinden.

Let op: Verwijderen is niet hetzelfde als vernietigen. Het verwijderen van verzamelde persoonsgegevens houdt in dat deze gegevens buiten het bereik van de actieve administratie worden gebracht en worden ondergebracht in een - al dan niet digitaal - archief. Van vernietigen is pas sprake als de gegevens nergens meer zijn opgeslagen.

3.6 Integriteit en vertrouwelijkheid

Integriteit en vertrouwelijkheid zijn twee begrippen die ook in paragraaf 2.3 aan de orde zijn gekomen bij informatiebeveiliging. Voor het privacybeleid wordt onder deze begrippen verstaan dat persoonsgegevens door passende technische of organisatorische maatregelen op een dusdanige manier verwerkt worden dat een passende beveiliging is gewaarborgd. Zodat betrokkenen er op kunnen vertrouwen dat er zorgvuldig wordt omgegaan met hun gegevens. De organisatorische en technische maatregelen om dit beginsel binnen de Nationale ombudsman te waarborgen komen in hoofdstuk 4 aan de orde.

3.7 Verantwoordingsplicht/Accountability

De verantwoordingsplicht is één van de belangrijkste verplichtingen van de AVG. Het betekent dat de Nationale ombudsman moet kunnen aantonen dat verwerkingen aan de regels van de AVG voldoen.

Het privacybeleid draagt bij aan deze verantwoordingsplicht. Hiermee toont de Nationale ombudsman aan dat er passende en effectieve interne processen en instrumenten aanwezig zijn. Zodat de principes en verplichtingen van gegevensbescherming kunnen worden nageleefd zodat betrokkenen voldoende beschermd zijn.

Daarnaast kan de Nationale ombudsman dit aantonen met het AVG-register.

De organisatorische en technische maatregelen om dit beginsel binnen de Nationale ombudsman te waarborgen komen in hoofdstuk 4 van deze notitie aan de orde.

4. Organisatorische en technische maatregelen privacybeleid

Ter waarborging van het privacybeleid treft de Nationale ombudsman verschillende organisatorische, technische en fysieke maatregelen die hieronder worden toegelicht. Deze maatregelen bieden de kaders en handvatten aan medewerkers van de Nationale ombudsman om op de gewenste wijze te kunnen handelen wanneer het gaat om persoonsgegevens. In deze paragraaf worden deze organisatorische en technische maatregelen nader toegelicht.

4.1 Aanstelling FG

In de AVG is het een verplichting geworden voor alle overheidsinstanties en publieke organisaties om een FG aan te stellen. De FG zorgt er voor dat het MT gevraagd en ongevraagd op de hoogte wordt gesteld van de naleving van het privacybeleid binnen de diensten van de Nationale ombudsman, en zorgt dat het MT op de hoogte is van risico's en misstanden. Voor uitgebreide omschrijving van de rol en taken van de FG wordt verwezen naar paragraaf 2.4.

4.2 Contactpersoon AVG per dienst

De AVG contactpersoon brengt het privacybeleid, in samenwerking met het diensthoofd, onder de aandacht van de medewerkers van de eigen dienst zodat het privacybewustzijn wordt vergroot en het privacybeleid geborgd is binnen alle diensten. Voor omschrijving van de rol en taken van de AVG contactpersoon wordt verwezen naar paragraaf 2.5.

4.3 AVG-register

Alle verwerkingen van persoonsgegevens worden opgenomen in het digitale AVG register. De gedachte hierachter is dat wanneer de documentatie niet op orde is, niet aangetoond kan worden dat zorgvuldig wordt omgegaan met de bescherming van persoonsgegevens. Bovendien kan in geval van incidenten (datalekken), een bezoek van de toezichthouder (Autoriteit Persoonsgegevens) of verzoeken van betrokkenen adequaat worden gehandeld. Het AVG-register wordt door elke onderdeel zelf gevuld, door de AVG-contactpersoon. De verantwoordelijke leidinggevende geeft per verwerking een definitief akkoord.

4.4 AVG-loket

De Nationale ombudsman waarborgt de rechten van betrokkenen en houdt persoonsgegevens juist en actueel. Er is een procedure ingericht om te zorgen dat betrokkenen hun rechten kunnen uitoefenen. Dit wordt duidelijk en transparant gecommuniceerd, zowel op het intranet als op het internet.

4.5 Procedure datalekken

Er kan sprake zijn van een datalek wanneer belangrijke documenten, gegevensbestanden of gegevensdragers als een telefoon of usb-stick zijn kwijtgeraakt of bijvoorbeeld onbedoeld zijn gepubliceerd. Om de gevolgen van datalekken voor betrokkenen te beperken en toezicht te kunnen houden op de juiste afhandeling van datalekken is een procedure datalekken opgesteld. Deze is te vinden op het intranet. Bovendien wordt een register bijgehouden van de (potentiële) datalekken en beveiligingsincidenten. Het doel van deze registratie is dat ervan kan worden geleerd, zodat datalekken in

de toekomst zoveel mogelijk worden voorkomen. Een ander doel is dat daarmee aan de Autoriteit Persoonsgegevens kan worden aangetoond dat datalekken daadwerkelijk worden gemonitord en opgevolgd.

4.6 Verwerkersovereenkomsten via Bestuursbureau (Inkoop)

Wanneer externe partijen (verwerkers) toegang hebben tot de persoonsgegevens moeten met deze externe partij onder andere afspraken gemaakt worden over de organisatorische en technische beveiliging van persoonsgegevens, de rechtmatigheid van de gegevensverwerking en het melden van datalekken bij de verwerkingsverantwoordelijke van de Nationale ombudsman. Deze afspraken worden opgenomen in een verwerkingsovereenkomst. Het Bestuursbureau beschikt over een standaard verwerkingsovereenkomst en kan hierbij adviseren.

4.7 Privacy Impact Assessment

De verwerkingsverantwoordelijke is verplicht een gegevensbeschermingseffectbeoordeling (GEB), ook wel genoemd een Privacy Impact Assessment (PIA), uit te voeren voor verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen (de betrokkenen). Er moet dan inzichtelijk worden gemaakt wat de impact van de verwerking is op de persoonlijke levenssfeer van betrokkenen, zodat door het treffen van maatregelen de risico's kunnen worden teruggebracht naar acceptabele grenzen. Bij elk nieuw project of systeem waarbij mogelijk risicovolle verwerkingen van persoonsgegevens zijn betrokken, zal een GEB/PIA worden afgenomen.

4.8 Interne/externe scholing

- FG moet voldoende kennis opbouwen en bijhouden
- FG zorgt dat AVG-contactpersonen voldoende kennis opbouwen en bijhouden
- FG zorgt dat medewerkers Nationale ombudsman voldoende kennis opbouwen en bijhouden

4.9 Interne en externe communicatie

Een transparante interne en externe communicatie door het Bestuursbureau van de Nationale ombudsman zorgt er voor dat alle betrokkenen op de hoogte zijn van het privacybeleid van de Nationale ombudsman en geïnformeerd zijn over hoe ze gebruik kunnen maken van hun rechten. Daarbij is het privacybeleid van de Nationale ombudsman vooral bedoeld om de interne organisatie te informeren. En zijn de privacyverklaringen en disclaimers vooral bedoeld om de buitenwereld te informeren. Zij zijn meer het visitekaartje naar buiten toe en informeren betrokken hoe zij gebruik kunnen maken van hun rechten en plichten.

Bijlage: verklaring van begrippen

- **Integrale beveiliging:** beveiliging van personen, gebouwen, terreinen, (gerubriceerde) informatie, privacy en integriteit.
- **Persoonsgegevens:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
- **We kennen vier vormen van privacy:**
 - **Informationele privacy:** gaat over het verwerken en verzamelen van persoonlijke data, bijvoorbeeld financiële gegevens, medische gegevens, contactgegevens etc.
 - **Territoriale privacy:** gaat over de persoonlijke omgeving van een individu en de grenzen die hierbij horen, bijvoorbeeld op werk, thuis en publieke ruimtes.
 - **Lichamelijke privacy:** gaat over de fysieke privacy van een persoon bijvoorbeeld genetische onderzoeken, drugstests, abortus etc.
 - **Communicatieve privacy:** gaat over de vrijheden rondom correspondentie via post, telefoongesprekken, e-mail etc.
- **Privacy Enhancing Technologies:** de term Privacy Enhancing Technologies (PET) wordt gehanteerd om alle ICT-middelen aan te duiden die gebruikt kunnen worden om persoonsgegevens te beschermen.
- **Gegevensbeschermingseffectbeoordeling (GEB/PIA):** een GEB/PIA is een risicoanalyse die een organisatie helpt om bij een nieuw project, proces of systeem in een vroeg stadium inzicht te krijgen in de privacyrisico's.
- **Verwerker:** een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, maar niet onder diens rechtstreekse gezag valt.
- **Verwerking:** een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens. Al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
- **Verwerkingsverantwoordelijke:** een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen

Beveiligingsmaatregelen voor Leveranciers

Versie 0.9

Beveiligingseisen <Systeem>	
Systeem:	<Betrokken Systeem, Dienst, Proces>
Dataclassificatie	<Datum Dataclassificatie>
Beschikbaarheid	<Laag, Midden, Hoog, Zeer Hoog>
Integriteit	<Laag, Midden, Hoog, Zeer Hoog>
Vertrouwelijkheid	<Laag, Midden, Hoog, Zeer Hoog>

Beveiligingsmaatregelen Leveranciers				
Nr	S/M*	Eis	Classificatie	Omschrijving hoe de leverancier invulling geeft aan de
1	M	Leverancier is ISO 27001 of NEN 7510 gecertificeerd.	Alle	Nvt
2	M	Leverancier overlegt jaarlijks het ISO 27001 of NEN 7510 certificaat en bijbehorende Verklaring van Toepasselijkheid.*	Alle	Nvt
3	S	Leverancier overlegt jaarlijks een Standaard/Richtlijn 3000 Type II verklaring.	Alle	Nvt
Indien aan bovenstaande eisen niet is voldaan zijn onderstaande punten van toepassing in plaats van optioneel. *) De Verklaring van Toepasselijkheid (VvT) wordt gecontroleerd of deze de overeengekomen dienstverlening afdekt.				
4	M	De leverancier beschikt over een informatiebeveiligingsbeleid.	Alle	
5	M	De leverancier onderhoudt het informatiebeveiligingsbeleid periodiek.	Alle	
6	S	De leverancier is bereid inzage te geven in het informatiebeveiligingsbeleid (na ondertekening van een geheimhoudingsverklaring).	BBN2 of hoger > Must	

7	M	De leverancier heeft de verantwoordelijkheden voor informatiebeveiliging formeel belegd in de organisatie.	Alle	
8	S	De leverancier is bereid het recht op het laten uitvoeren van een audit op te nemen in de overeenkomst.	BBN2 of hoger > Must	
9	M	De leverancier zal alle bedrijfsinformatie van de Nationale ombudsman geheimhouden en niets daarover openbaar maken zonder schriftelijke toestemming van de Nationale ombudsman.	Alle	
10	M	De leverancier heeft in het personeelsbeleid bepalingen voor informatiebeveiliging opgenomen waar al het personeel voor akkoord heeft getekend.	BBN2 of hoger > Must	
11	S	De leverancier beschikt over een dataclassificatiebeleid	BBN2 of hoger > Must	
12	S	De leverancier labelt alle informatie en heeft beleid hoe informatie per classificatie behandeld moet worden	BBN2 of hoger > Must	
13	S	De leverancier beschikt over beleid m.b.t. fysieke beveiligingsmaatregelen.	BBN2 of hoger > Must	
14	M	De leverancier verstrekt haar personeel richtlijnen over acceptabel gebruik van informatievoorzieningen.	Alle	
15	M	De leverancier past een clear screen en clear desk beleid toe.	Alle	
16	M	De leverancier heeft beleid en maatregelen die bescherming biedt tegen malware.	Alle	
17	M	De leverancier voorziet haar systemen en werkplekken tijdig van (security)updates.	Alle	
18	S	De leverancier benoemt informatiebeveiliging in elk project (Security by Design).	BBN2 of hoger > Must	

19	M	De leverancier staat er voor in dat (ingehuurd) personeel van de leverancier de bepalingen betreffende gedrag, vertrouwelijkheid en bescherming van gegevens naleven	Alle	
20	S	De leverancier voert een screeningbeleid voor nieuw personeel.	BBN2 of hoger > Must	
21	M	Medewerkers van de leverancier die werkzaamheden uitvoeren of informatie verwerken van de Nationale ombudsman overleggen voor aanvang van de werkzaamheden bij de organisatie een recente Verklaring Omtrent het Gedrag (VOG) met een screeningsprofiel gerelateerd aan de werkzaamheden. De leverancier stemt voorafgaand aan de aanvraag de noodzaak, inhoud en aard hiervan af met de organisatie.	V=Midden of hoger	
22	S	Medewerkers van de leverancier worden periodiek getraind op het gebied van Security Awareness.	BBN2 of hoger > Must	
23	M	De leverancier dwingt Multi Factor Authenticatie af voor alle toegang vanaf onvertrouwde netwerken (internet) tot het bedrijfsnetwerk.	Alle	
24	M	De leverancier heeft maatregelen genomen om aan het einde van het dienstverband van het personeel alle toegang tot informatie van de Nationale ombudsman in te trekken.	Alle	
25	M	Aan het einde van de overeenkomst draagt de leverancier alle data over aan de Nationale ombudsman en na de bevestiging van ontvangst wordt alle data vernietigd door de leverancier.	Alle	

#VERW!	M	Alle informatie van de Nationale ombudsman die de leverancier opslaat is met toegangsbeveiliging en encryptie beveiligd. De encryptie voldoet aan de richtlijnen van Forum Standaardisatie en/of het NCSC	BBN2 of hoger > Must	
#VERW!	M	De leverancier garandeert dat alle informatie van de Nationale ombudsman die opslaat uitsluitend toegankelijk is voor medewerkers van de leverancier die een 'need-to-know' hebben in de dienstverlening aan de Nationale ombudsman	BBN2 of hoger > Must	
#VERW!	M	De leverancier voert een actief toegangsbeveiligingsbeleid met periodieke controles** voor alle systemen m.b.t. de Nationale ombudsman.	BBN2 of hoger > Must ** Voor BBN 3 een frequentie van eens per kwartaal of vaker.	
#VERW!	M	De leverancier logt en monitort actief alle handelingen m.b.t. toegang tot informatie van de Nationale ombudsman	BBN2 of hoger > Must	
#VERW!	M	De leverancier maakt back-ups zoals in de SLA is overeengekomen. De leverancier controleert minimaal maandelijks met een Restore test of de backups daadwerkelijk terug te zetten zijn. (Een verzoek van de Nationale ombudsman voor een restore mag aangemerkt worden als restore test)	BBN2 of hoger > Must	
#VERW!	S	De leverancier gebruikt een Secure Software Development methode voor het ontwikkelen van toepassingen voor de Nationale ombudsman	Indien van toepassing	
#VERW!	S	De leverancier laat periodiek een onafhankelijke partij een controle uitvoeren op de beveiliging van de applicaties en organisatie.	BBN2 of hoger > Must	
#VERW!	M	De leverancier gebruikt geen (Nationale ombudsman) Productiegegevens om te testen.	Alle	

#VERW!	M	De leverancier stelt eisen voor informatiebeveiliging aan haar leveranciers (die betrokken zijn bij de dienstverlening aan de Nationale ombudsman en beoordeelt deze periodiek.	Alle	
#VERW!	M	De leverancier heeft een Incident Management proces waarbij informatiebeveiligingsincidenten gemeld, beoordeeld en opgevolgd worden. Wanneer informatie of systemen van de Nationale ombudsman hierbij betrokken zijn wordt de Nationale ombudsman hierover geïnformeerd.	Alle	
#VERW!	M	In het geval van afnemen van producten en/of diensten accepteert de leverancier dat (beveiligings)incidenten direct worden gemeld aan de Nationale ombudsman	Alle	
#VERW!	S	De leverancier beschikt over een Informatiebeveiligingscontinuïteitplan en test dit periodiek	BBN2 of hoger > Must	
#VERW!	M	De leverancier verstrekt uitsluitend toegang tot systemen en informatie van de Nationale ombudsman aan eigen werknemers.	Alle	
#VERW!	M	De Leverancier legt alle beveiligingseisen van de Nationale ombudsman ook op aan onderaannemers die betrokken zijn bij de dienstverlening van de Nationale ombudsman	Alle	
#VERW!	S	De beoordeling op SSL Labs van de website(s) betrokken bij de dienstverlening scoren een A of hoger	BBN2 of hoger > Must	

*) Should of Must

**) Beschrijving beveiligingsmaatregel bij de leverancier in te vullen door de Information Security Officer van de leverancier

Privacymaatregelen voor Leveranciers

Versie 0.9

Privacymaatregelen Leveranciers				
Nr	S/M*	Eis	Classificatie	Omschrijving hoe de leverancier invulling geeft aan de gevraagde
1	S	Leverancier is BC5701 (AVG) gecertificeerd.		Nvt
2	S	Leverancier overlegt jaarlijks het BC5701 certificaat en		Nvt
Indien aan bovenstaande eisen niet is voldaan zijn onderstaande punten van toepassing in plaats van optioneel. *) De Verklaring van Toepasselijkheid (VvT) wordt gecontroleerd of deze de overeengekomen dienstverlening afdekt.				
3	M	De leverancier beschikt over een privacybeleid.		
4	M	De leverancier onderhoudt het privacybeleid periodiek.		
5	S	De leverancier is bereid inzage te geven in het privacybeleid (na ondertekening van een geheimhoudingsverklaring).		
6	M	De leverancier beschikt over een verwerkingsregister en heeft		
7	S	De leverancier laat periodiek een audit door een onafhankelijke partij uitvoeren en is bereid de resultaten te delen met de		
8	M	Medewerkers van de leverancier ontvangen periodiek privacy		
9	M	De leverancier verwerkt geen persoonsgegevens buiten de EER.		
10	M	De leverancier informeert de No vooraf bij het aangaan van een overeenkomst met een nieuwe subverwerker.		
11	M	De leverancier heeft toestemming nodig van de No om een overeenkomst aan te gaan met een nieuwe subverwerker.		
12	M	De leverancier legt alle verplichtingen uit de		
13	M	De leverancier beschikt over een datalekprotocol/procedure.		
14	M	De leverancier meldt (vermoedelijke) datalekken aan de Nationale ombudsman zonder onredelijke vertraging zodra hij ervan kennis		
15	S	De leverancier hanteert privacy by design als uitgangspunt bij		
16	M	De leverancier neemt passende technische en organisatorische maatregelen om persoonsgegevens te beschermen en kan dit ook		

17	M	Medewerkers in dienst van, of handelend in opdracht van, de leverancier hebben een geheimhoudingsplicht.		
18	M	De technische en organisatorische maatregelen, die als bijlage onderdeel zijn van de verwerkersovereenkomst, zijn actueel		
19	M	Het overzicht van subverwerkers is actueel		
20	M	De leverancier kan aantonen hoe en de wijze waarop de rechten		
	M	De leverancier verstrekt, na beëindiging van het contract tussen leverancier en de Nationale ombudsman, op verzoek alle gegevens in het systeem. De leverancier behoudt de gegevens zelf niet.		

*) Should of Must

**) Beschrijving privacymaatregel bij de leverancier in te vullen door de Privacy Officer of FG van de leverancier

Privacymaatregelen voor Leveranciers

Versie 0.9

Privacymaatregelen Leveranciers				
Nr	S/M*	Eis	Classificatie	Omschrijving hoe de leverancier invulling geeft aan de gevraagde
1	S	Leverancier is <ISO> gecertificeerd.		
2	S	Leverancier overlegt jaarlijks het <ISO> certificaat en bijbehorende		
Indien aan bovenstaande eisen niet is voldaan zijn onderstaande punten van toepassing in plaats van optioneel. *) De Verklaring van Toepasselijkheid (VvT) wordt gecontroleerd of deze de overeengekomen dienstverlening afdekt.				
3	M	De leverancier beschikt over een AI beleid.		
4	M	De leverancier onderhoudt het AI beleid periodiek.		
5	S	De leverancier is bereid inzage te geven in het AI beleid (na ondertekening van een geheimhoudingsverklaring).		
6	S	De leverancier laat periodiek een AI audit door een onafhankelijke partij uitvoeren en is bereid de resultaten te delen met de Nationale		
7	M	De technische en organisatorische maatregelen, die als bijlage onderdeel zijn van de verwerkersovereenkomst, zijn actueel		

*) Should of Must



nationale ombudsman

Beleid

Informatiebeveiliging en Privacy Bewustzijn

2024-2026

Document classificatie
Vertrouwelijk

Versienummer	1.0
Eigenaar	Informatieregie \ CISO & FG
Opgesteld door	ISO/PO
Status	Definitief
Vastgesteld door	CIO overleg
Vastgesteld op datum	12-09-2024
Datum eerste versie	21-02-2024
Laatst bijgewerkt	18-09-2024

Versiebeheer

Datum	Versie	Aangepast door	Omschrijving/aanpassing
21-02-2024	0.1		Eerste opzet
07-03-2024	0.2		Review
12-06-2024	0.3		Verwerken feedback CISO/FG
01-08-2024	0.3		Review
15-08-2024	0.4		Verwerken feedback 
29-08-2024	0.5		Verwerken laatste feedback
06-09-2024	0.9		Gereed voor CIO.
12-09-2024	0.9	CIO overleg	Vastgesteld
18-09-2024	1.0		Definitief gemaakt na vaststelling, omgezet in pdf

1	INLEIDING	4
1.1	DOELSTELLING INFORMATIEBEVEILIGING & PRIVACY AWARENESS BELEID.....	4
1.2	SCOPE	5
1.3	VERANTWOORDELIJKHEID	5
1.4	RELATIE OVERIGE BELEIDSDOCUMENTEN	5
2	UITGANGSPUNTEN INFORMATIEBEVEILIGING & PRIVACY AWARENESS BELEID	6
3	PRAKTISCHE UITGANGSPUNTEN INFORMATIEBEVEILIGING & PRIVACY AWARENESS BELEID.....	7
3.1	INFORMATIEBEVEILIGING & PRIVACY AWARENESS ONBOARDING TRAJECT	7
3.2	OP PEIL BRENGEN KENNISNIVEAU	8
4	CONTROLE OP HET BELEID	10
4.1	O-METING	10
4.2	N-METING.....	10
4.3	RAPPORTAGES N.A.V. TRAININGEN, PHISHINGCAMPAGNES, QUIZZES, WEBINARS.....	10

1 Inleiding

De ombudsman¹ heeft veel technische en organisatorische maatregelen genomen om het risico van een informatiebeveiligingsincident zo klein mogelijk te maken. Ondanks deze set aan maatregelen blijft er een component dat heel essentieel is in de keten van informatiebeveiliging en privacy: de mens.

Het juist handelen van een medewerker kan een groot beveiligings- en privacy incident (hierna te noemen **incident**) voorkomen. Maar omgekeerd is ook mogelijk, bij verkeerd handelen kan er juist een incident ontstaan.

Het is daarom belangrijk om de medewerkers goed te trainen om zo een waardevolle extra beveiligingslaag te creëren. Dit is niet een eenmalige training maar vergt continue aandacht om het gezamenlijke niveau van de organisatie hoog te houden.

1.1 Doelstelling Informatiebeveiliging & Privacy Awareness Beleid

Het doel van dit Informatiebeveiliging & Privacy Awareness beleid is een werkwijze te definiëren waarmee het bewustzijn van alle medewerkers verhoogd wordt en op een hoog niveau gehouden wordt. Zo zijn de medewerkers op de hoogte van informatiebeveiligingsrisico's, privacy kwesties, de gedragsregels en beveiligingsmaatregelen. Het beleid helpt bij het creëren en behouden van een gezonde en goede IT veiligheidscultuur binnen de ombudsman.

Om het bewustzijnsniveau van de organisatie te meten zijn de volgende KPI's opgesteld:

1. **Betrokkenheid bij security & privacy training:** 75% van de werknemers neemt deel aan de security & privacy awareness trainingen binnen een bepaalde periode.
2. **Phishing simulatie succes ratio:** 90% van de werknemers doorstaat succesvol een phishing simulaties zonder te klikken op kwaadaardige links of bijlagen.
3. **Percentage Awareness (bewustzijn):** 85% van de medewerkers vertoont voldoende kennis of begrip van de relevante informatie, procedures of richtlijnen. "voldoende" wordt gedefinieerd in het plan van aanpak van het programma.
4. **Gemiddelde tijd om incidenten te rapporteren:** minder dan 2 uur nodig om incidenten te melden op de correcte manier.
5. **Succescriteria voor beleid en resultaten:** Mate van naleving van beleidsmaatregelen door werknemers, gemeten aan de hand van interne audits of enquêtes.

Met het opstellen van het Informatiebeveiliging & Privacy Awareness beleid wordt invulling gegeven aan het volgende hoofdstuk van de Baseline Informatiebeveiliging Overheid (BIO).

- 7.2.2: Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Tevens wordt op het gebied van Privacy invulling gegeven aan de volgende hoofdstukken van de AVG:

- Artikel 39, lid 1b "...Bewustmaking en opleiding van het bij de verwerking betrokken personeel..."

¹ ombudsman omvat de Nationale ombudsman, de Kinderombudsman en de Veteranenombudsman.

1.2 Scope

Het Informatiebeveiliging & Privacy Awareness beleid is van toepassing op alle medewerkers in vaste of tijdelijke dienst, stagiaires en externen die voor of namens de ombudsman toegang hebben tot de informatievoorziening en ICT-middelen van de ombudsman.

1.3 Verantwoordelijkheid

Dit beleid wordt minimaal één keer per drie jaar herzien of wanneer er grote wijzigingen zijn vanuit de organisatie c.q. overheid, aangepast en opnieuw goedgekeurd. In de review wordt specifiek rekening gehouden met de effectiviteit van het beleid. Bij het publiceren van het nieuwe beleid wordt gecommuniceerd wat de wijzigingen t.o.v. de vorige versie zijn.

De Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) zijn verantwoordelijk voor het onderhoud van dit beleid. Het lijnmanagement is verantwoordelijk voor het toepassen van dit beleid binnen hun verantwoordingsgebied.

1.4 Relatie overige beleidsdocumenten

De volgende documenten hebben een relatie met dit beleidsdocument:

- Informatiebeveiligingsbeleid 2024-2026
- Privacy beleid
- Risicomanagement beleid
- Overige documenten

2 Uitgangspunten Informatiebeveiliging & Privacy Awareness beleid

Bij de toepassing van het Informatiebeveiliging & Privacy Awareness beleid binnen de ombudsman worden de volgende uitgangspunten gehanteerd:

- Informatiebeveiliging & Privacy Awareness is een essentieel onderdeel van de set aan beveiligingsmaatregelen van de ombudsman.
- De ombudsman is zich bewust dat een medewerker zowel een incident kan voorkomen als veroorzaken.
- Het Informatiebeveiliging & Privacy Awareness beleid is gericht op het proactief trainen van werknemers over potentiële beveiligingsrisico's en het belang van het beschermen van gevoelige informatie waaronder persoonsgegevens.
- Het Informatiebeveiliging & Privacy Awareness beleid is gericht op het bevorderen van een cultuur waarin medewerkers het belangrijk vinden om zich in te zetten ten aanzien van protocollen en -kwesties omtrent informatiebeveiliging en privacy.
- De ombudsman stelt de benodigde mensen en middelen beschikbaar om haar medewerkers te trainen zoals gesteld in dit beleid.
- Het lijnmanagement is verantwoordelijk dat iedere medewerker, zowel vast als tijdelijk, intern of extern, deelneemt aan de genomen Informatiebeveiliging & Privacy awareness maatregelen.
- Periodiek wordt gecontroleerd of de gestelde doelen gehaald zijn en wordt er bijgestuurd wanneer de gedefinieerde doelen niet gehaald zijn.

3 Praktische uitgangspunten Informatiebeveiliging & Privacy Awareness beleid

Informatiebeveiliging & Privacy Awareness bij de ombudsman bestaat uit twee delen. Een basis deel om de kennis op peil te houden dat periodiek wordt toegepast en een projectmatige aanpak voor gedragsverandering.

3.1 Informatiebeveiliging & Privacy Awareness onboarding traject

Informatiebeveiliging & Privacy Awareness begint al bij de on-boarding van nieuwe medewerkers. Onderdeel van het proces voor de indiensttreding is het verstrekken van de benodigde informatie over informatiebeveiliging en privacy. Tijdens de onboardingsperiode krijgen alle nieuwe medewerkers belangrijke informatie over het (veilig) werken bij de nationale ombudsman. In een presentatie wordt uitgelegd wat het belang is van informatiebeveiliging en privacy bij de ombudsman, wie daarbij betrokken zijn, welke informatie wij verwerken en wat wij van onze medewerkers verwachten. Kortom, wat verstaan wij onder informatiebeveiliging en privacy.

3.1.1 Kennisniveau op peil houden

Is eenmaal de basis gelegd met de onboarding wordt periodiek het kennisniveau op peil gehouden. De scope is hier groter dan alleen de nieuwe medewerkers, ook de medewerkers die al langer in dienst zijn worden hiermee bereikt.

Op basis van de bovenstaande elementen maakt de Chief Information Security Officer samen met de Functionaris Gegevensbescherming een informatiebeveiliging & Privacy Awareness plan met daarin de bewustzijnsactiviteiten om het kennisniveau van de medewerkers op peil te houden. Jaarlijks wordt vastgesteld welke activiteiten op dit gebied aan de medewerkers zullen worden aangeboden en in welke mate dit verplicht of vrijwillig is.

Voor het op peil houden van het niveau worden de doelen voor de campagne gevoed met de volgende elementen:

- Slecht of matig scorende elementen uit de voorgaande Informatiebeveiliging & Privacy Awareness campagnes;
- Incidenten bij de ombudsman uit de afgelopen periode;
- Nieuwe dreigingen (NCSC Cybersecurity Beeld Nederland 2023, digitaleoverheid.nl);
- Wijzigingen in beleid en/of relevante wet- en regelgeving;
- Thema's/ontwikkelingen die spelen of gaan spelen bij de ombudsman (Artificial intelligence (AI), NIS2).

3.1.2 Oktober Cybersecuritymaand

Elk jaar wordt in oktober, de Cybersecuritymaand, een speciale campagne gestart om informatiebeveiliging en privacy extra onder de aandacht te brengen. Gedurende de hele maand is hier extra aandacht voor. Dit wordt gecombineerd met campagneonderdelen om de medewerkers ook actiever te betrekken.

Verder wordt vanuit de Rijksoverheid ([Digitale Overheid](https://digitaleoverheid.nl)) en het Nationaal Cyber Security Centrum (NCSC) verschillende activiteiten geboden zoals webinars, congressen, demo's en workshops, waarop ingehaakt kan worden

3.1.3 Overige maatregelen

Om het kennisniveau van de medewerkers op peil te houden zijn er nog tal van andere maatregelen die georganiseerd kunnen worden, zoals het uitnodigen van een gastspreker, hacker of pentester. Ook het initiatief 'Rondje lang de teams' is een maatregel waarbij de afdelingen die geïnteresseerd zijn in meer informatie over informatiebeveiliging en privacy bij de Information Security Officer en Privacy Officer terecht kunnen. De Information Security Officer en/of Privacy Officer organiseren presentaties om relevante informatie over te dragen en zo de bewustwording te vergroten.

De Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) bepalen welke overige maatregelen ingezet moeten worden om het kennisniveau op peil te houden.

3.2 Op peil brengen kennisniveau

Vanwege de technologische en organisatorische ontwikkelingen is het belangrijk om het kennisniveau op peil te brengen. Met het **Informatiebeveiliging & Privacy Awareness programma** trainen we alle medewerkers op het gebied van informatieveiligheid, veilig werken, AVG en privacy in het dagelijks werk. De te halen verbeteringen ten opzichte van het vorige traject liggen met name op:

- Betere participatie
- Meetbaar en inzichtelijk maken van het effect van het trainen.
- Geen gebruik maken van een standaard e-learning tool.
- Wel gebruik maken van eigen scenario's en modules passend bij het dagelijks werk in deze organisatie

De ombudsman wil hiermee het kennis- en gedragsniveau op het gebied van informatieveiligheid en privacy bij haar medewerkers verhogen zodat zij veilig werken en waakzaam zijn. Tevens is het belangrijk dat de medewerkers verdachte situaties herkennen en in dat geval weten wat ze moeten doen. Om dit te bereiken is het nodig dat:

- De medewerker weet en snapt waar de risico's liggen.
- De medewerker verschillende soorten aanvalsmethodes herkent.
- De medewerker weet wat de veilige manier van werken is.
- De medewerker goed uitgerust wordt om op een veilige manier te werken.
- De medewerker weet bij wie of waar hij/zij/hen terecht kan bij vragen of twijfels en zich daarbij veilig voelt.
- Er een cultuur is van elkaar helpen en samen leren.

Het Informatiebeveiliging & Privacy Awareness programma bestaat uit phishing simulaties, webinars en quizen. De medewerkers zijn verplicht om hieraan deel te nemen. Met het security awareness programma hebben we als doelstelling om:

1. Minstens één phishing 0 fails krijgen
2. Minstens één phishing 40% van de medewerkers die een simulatie herkennen en hier een melding van maken
3. Participatiegraad van 85% bij de webinars
4. Security Awareness Proficiency Assessment score verbeteren:
 - a. Participatiegraad van 75% of meer
 - b. Verbetering op de onderdelen: Wachtwoorden en authenticatie, Sociale Media, Human Firewall / incidenten rapporteren en Kennisvragen AVG/privacy

Aan het einde van een Informatiebeveiliging & Privacy Awareness Programma vindt een evaluatie plaats. Wanneer mogelijk wordt de directie middels de managementrapportages op de hoogte gehouden van de voortgang van de campagne. De Chief Information Security Officer en Functionaris Gegevensbescherming zijn verantwoordelijk voor het programma.

4 Controle op het beleid

De CISO en de FG zijn verantwoordelijk voor de controle op de werking van dit beleid, dit zullen zij o.a. doen door middel van:

4.1 0-meting

Het doel van de 0-meting is gericht om een baseline vast te stellen. De 0-meting levert waardevolle inzichten op in de bestaande kennis, houding en gedrag op het gebied van informatiebeveiliging en privacy binnen onze organisatie. Door deze gegevens te analyseren, kunnen we verbeterpunten identificeren en gerichte acties ondernemen om de effectiviteit van onze Informatiebeveiliging & Privacy Awareness campagnes te vergroten. Op basis van nulmetingen streven we ernaar een cultuur van voortdurende verbetering te bevorderen en een sterke bescherming van onze gevoelige informatie te garanderen.

4.2 N-meting

In de n-meting (gebruikelijk een 2e en/of 3e) wordt de progressie op de gestelde doelen bepaald. Deze meting wordt uitgevoerd om de voortgang te evalueren en gebruikt om de huidige campagne bij te stellen of dient als input voor de volgende campagne.

4.3 Rapportages n.a.v. trainingen, phishingcampagnes, quizzes, webinars

Na afloop van een campagne (onderdeel) worden rapportages verstuurd aan de CISO en de FG. Deze rapportages geven inzicht in welke mate het kennisniveau is verhoogd en de gewenste gedragsverandering is geborgd in de organisatie.

Op basis van de bevindingen worden gerichte actiepunten vastgesteld om de effectiviteit van de campagne te verbeteren. Deze actiepunten omvatten onder meer het implementeren van aanvullende trainingen, het updaten van beleidsrichtlijnen en procedures en het versterken van de beveiligingsmaatregelen. De keuze voor toekomstige campagnes worden gebaseerd op de score uit de rapportages.



nationale ombudsman

Beleid

Informatiebeveiliging en Privacy bij leveranciersrelaties

2024-2026

Document classificatie

Vertrouwelijk

Versienummer	1.0
Opgesteld door	[redacted] J, [redacted] J, [redacted] J
Eigenaar	Informatieregie \ CISO
Status	Definitief
Vastgesteld door	CIO overleg
Vastgesteld op datum	12-09-2024
Datum eerste versie	20-01-2022
Laatst bijgewerkt	18-09-2024

Versiebeheer

Datum	Versie	Aangepast door	Omschrijving/aanpassing
24-04-2024	0.4	[redacted] J	Privacy opgenomen en opmerkingen [redacted] J verwerkt
30-05-2024	0.5	[redacted] J	- P samengevoegd met IB in H3; - Assurance-rapportage type 2 toegevoegd naast de reeds vereiste certificeringen; - H5.1 periodieke controles uitgewerkt; en - gehele tekst aangescherpt.
08-07-2024	0.9	[redacted] J	Review en enkele aanpassingen tav frequentie rapportages en overleggen, alsmede uitvoering van periodieke controle van onderleveranciers.
30-08-2024	0.91	[redacted] J	Review.
05-09-2024	0.92	[redacted] J	Reviews [redacted] J, [redacted] J verwerkt
[redacted] J	0.92	[redacted] J	Gereed voor CIO.
12-09-2024	0.92	CIO Overleg	Vastgesteld
18-09-2024	1.0	[redacted] J	Definitief gemaakt na vaststelling, omgezet in pdf

Inhoudsopgave

1	INLEIDING	3
1.1	TOELICHTING	3
1.2	DOELSTELLING	3
1.3	SCOPE	3
1.4	VERANTWOORDELIJKHEDEN.....	3
1.5	RAAKVLAK BIO- NORMENKADER.....	3
1.6	RAAKVLAK AVG ARTIKELN	4
1.7	ONDERSTEUNENDE DOCUMENTATIE	4
1.8	RELATIE OVERIGE BELEIDSDOCUMENTEN INFORMATIEBEVEILIGING	4
2	UITGANGSPUNTEN	5
3	VOORAFGAAND AAN DE OVEREENKOMST.....	6
3.1	TOETSING OP BEVEILIGINGSMAATREGELEN EN PRIVACYMAATREGELEN LEVERANCIERS	6
3.1.1	Certificering / Assurance	7
3.1.2	Specifiek	7
3.1.3	Combinatie.....	8
3.2	BEOORDELING.....	8
3.2.1	Verificatie.....	8
3.2.2	Non compliant.....	9
4	TIJDENS DE LOOPTIJD VAN DE OVEREENKOMST	10
4.1	PERIODIEKE RAPPORTAGE	10
4.2	PERIODIEKE OVERLEGGEN	10
4.3	PERIODIEKE CONTROLE	11

1 Inleiding

1.1 Toelichting

De ombudsman (Nationale ombudsman, Veteranenombudsman, Kinderombudsman) hecht groot belang aan informatiebeveiliging en privacy. Ook wanneer delen van de bedrijfsvoering zijn uitbesteed aan externe leveranciers blijft de ombudsman verantwoordelijk voor informatiebeveiliging en privacy. Daarom zal de informatiebeveiliging en privacy minimaal van hetzelfde niveau moeten zijn en blijven als wanneer de ombudsman het proces, systeem of dienst zelf volledig had beheerd. In dit beleid voor Leveranciersmanagement is beschreven hoe de ombudsman invulling geeft aan haar verantwoordelijkheid indien leveranciers worden ingeschakeld voor het leveren van producten en/of diensten.

1.2 Doelstelling

Deze richtlijn heeft tot doel te beschrijven hoe de informatiebeveiligings- en privacymaatregelen die voor de ombudsman gelden ook doorgezet worden naar leveranciers en hoe deze onderhouden en gecontroleerd worden.

1.3 Scope

Het beleid voor Informatiebeveiliging en Privacy in Leveranciersrelaties is van toepassing op alle ICT-dienstverlening die de ombudsman heeft uitbesteed. Het bestrijkt de informatiebeveiligings- en privacyaspecten van Leveranciersmanagement.

1.4 Verantwoordelijkheden

Team Informatieregie is verantwoordelijk voor het aangaan van overeenkomsten bij het afnemen van ICT-dienstverlening en alle afstemming om tot dat moment te komen. Daarbij is Team Informatieregie ook verantwoordelijk voor het uitvoeren en onderhouden van de maatregelen zoals beschreven in dit beleid.

De Chief Information Security Officer is verantwoordelijk voor het onderhoud van dit beleid.

Deze richtlijn wordt minimaal één keer per jaar gereviewd, aangepast en opnieuw goedgekeurd. In de review wordt specifiek rekening gehouden met de effectiviteit van de richtlijn.

Bij het publiceren van het nieuwe beleid wordt gecommuniceerd wat de wijzigingen t.o.v. de vorige versies zijn.

1.5 Raakvlak BIO- normenkader

Met het opstellen van het beleid voor Leveranciersmanagement wordt invulling gegeven aan de volgende hoofdstukken van de Baseline Informatiebeveiliging Overheid (BIO):

- 14.1.1: Analyse en specificatie van informatiebeveiligingseisen;
- 15.1.1: Informatiebeveiligingsbeleid voor leveranciersrelaties;
- 15.1.2: Opnemen van beveiligingsaspecten in leveranciersovereenkomsten;
- 15.1.3: Toeleveringsketen van informatie- en communicatietechnologie;
- 15.2.1: Monitoring en beoordeling van dienstverlening van leveranciers;
- 15.2.2: Beheer van veranderingen in dienstverlening van leveranciers.

1.6 Raakvlak AVG artikelen

Dit beleid geeft invulling aan de volgende hoofdstukken van de AVG:

- Hoofdstuk III: Rechten van betrokkenen:
 - Afdeling 1: Transparantie en regelingen
 - Afdeling 2: Informatie en toegang tot persoonsgegevens
 - Afdeling 3: Rectificatie en wissing van gegevens
 - Afdeling 4: Recht van bezwaar en geautomatiseerde individuele besluitvorming
 - Afdeling 5: Beperkingen
- Hoofdstuk IV: Verwerkingsverantwoordelijke en verwerker
 - Afdeling 1: Algemene verplichtingen
 - Afdeling 2: Persoonsgegevensbeveiliging
 - Afdeling 3: Gegevensbeschermingseffectbeoordelingen en voorafgaande raadpleging
 - Afdeling 5: Gedragscodes en certificering
- Hoofdstuk V: Doorgiften van persoonsgegevens aan derde landen of internationale organisaties

1.7 Ondersteunende documentatie

Dit beleid is gebaseerd op:

- Strategisch Informatiebeveiligingsbeleid Nationale Ombudsman 2020 t/m 2023 versie 1.0
- Risicomanagement bij de Nationale Ombudsman versie 1.0
- Privacybeleid

1.8 Relatie overige beleidsdocumenten informatiebeveiliging

De volgende documenten hebben een relatie met dit beleid:

- Bijlage Informatiebeveiliging en privacy in Leveranciersmanagement - Ombudsman

2 Uitgangspunten

Bij de toepassing van Informatiebeveiliging en Privacy voor Leveranciersrelaties binnen de ombudsman worden de volgende uitgangspunten gehanteerd:

- De beveiligingseisen zijn gebaseerd op de classificatie van het betrokken systeem of proces;
- Alle beveiligings- en privacyeisen die voor de ombudsman gelden worden ook opgelegd aan een leverancier voor de uitbestede diensten;
- Deze eisen worden ook doorgezet door de leverancier aan haar sub-leveranciers;
- Voor het aangaan van een overeenkomst is met de leverancier afgestemd aan welke beveiligings- en privacyeisen zij moet voldoen;
- Voor het aangaan van een overeenkomst zijn de beveiligings- en privacyeisen getoetst;
- De leverancier heeft bevestigd dat zij voldoen aan alle beveiligings- en privacyeisen van de ombudsman;
- De beveiligings- en privacyeisen zijn opgenomen in de contractuele afspraken met de leverancier;
- De leverancier rapporteert periodiek over informatiebeveiliging en bescherming van persoonsgegevens;
- De ombudsman voert periodiek overleg met leverancier over informatiebeveiliging en privacy bij de dienstverlening van leverancier.

3 Voorafgaand aan de overeenkomst

Voordat een overeenkomst met een leverancier afgesloten kan worden is het van belang dat alle informatiebeveiligings- en privacyeisen van de ombudsman ook aan de nieuwe leverancier opgelegd kunnen worden. Hiervoor wordt samen met de afdeling Inkoop de beveiligings- en privacyeisen opgesteld die met de (potentiële) leveranciers gedeeld kunnen worden. Deze eisen (maatregelen) zijn gebaseerd op de classificatie van het systeem of proces dat bij de leverancier afgenomen gaat worden. In Bijlage 'Informatiebeveiliging en privacy in leveranciersrelaties' is een lijst opgenomen met de basis eisen die aan de leverancier gesteld worden. Deze lijst wordt op basis van de classificatie specifiek gemaakt voor de betreffende leverancier zodat deze met hen gedeeld kan worden.

3.1 Toetsing op beveiligingsmaatregelen en privacymaatregelen leveranciers

De lijst 'Informatiebeveiliging- en privacymaatregelen leveranciers' zoals opgenomen in de Bijlage "Informatiebeveiliging en privacy bij Leveranciersrelaties - Ombudsman" beschrijft alle beveiligings- en privacymaatregelen die de ombudsman van haar leveranciers én onderleveranciers vereist alvorens een contract overeen wordt gekomen. De lijst kan op drie manieren ingezet worden:

1. Certificering / Assurance
 - Wanneer de leverancier beschikt over de ISO 27001 of NEN 7510 certificering voor informatiebeveiliging, de BC5701 certificering voor privacy en/of een relevant assurance-rapportage Standaard/Richtlijn 3000 type 2 met informatiebeveiliging en privacy in scope van het assurance-onderzoek, wordt de lijst 'Informatiebeveiliging en privacy maatregelen Leveranciers' vergeleken met de scope en beschrijving van de certificeringen en/of het assurance-rapport. De leverancier voldoet aan alle vereisten als volgens de certificeringen en/of het assurance-rapport de vereiste informatiebeveiliging- en privacymaatregelen afdoende zijn geïmplementeerd.
2. Specifiek
 - Wanneer de leverancier niet over de certificeringen voor informatiebeveiliging en privacy beschikt, kan deze nog steeds voldoen aan alle beveiligingseisen die de ombudsman stelt. In dergelijke gevallen wordt een 'right to audit' clause opgenomen in het contract en wordt de lijst 'Informatiebeveiliging- en privacymaatregelen leveranciers' gebruikt als object van onderzoek. De leverancier moet aan de ombudsman aantoonbaar kunnen maken dat zij de vereiste maatregelen afdoende heeft geïmplementeerd.
3. Combinatie
 - Wanneer een certificering niet voldoende zekerheid geeft of de risico's voor de ombudsman groot zijn kan een combinatie van beide gebruikt worden om nog meer zekerheid te krijgen dat de beveiligingseisen van de ombudsman goed overeenkomen met die van de leverancier.

Voor het bepalen wat de meest geschikte manier om de beveiligingsmaatregelen bij de leverancier op te leggen en te controleren wordt onderstaande richtlijn gehanteerd:

Hoogste classificatie	Classificatie	Leverancier gecertificeerd	Leverancier niet gecertificeerd
BBN 1	0 + 1	Optioneel (Certificering)	Optioneel (Specifiek)
BBN 2	2	Certificering, Specifiek optioneel	Specifiek

BBN 2+	3	Certificering + Specifiek	Leverancier uitgesloten
BBN 3	3	Certificering + Specifiek	Leverancier uitgesloten

3.1.1 Certificering / Assurance

De ombudsman heeft de voorkeur om diensten uit te besteden aan partijen die ISO 27001 gecertificeerd zijn, en/of een assurance-rapportage Standaard/Richtlijn 3000 type 2 met informatiebeveiliging en privacy in scope van het assurance-onderzoek kunnen overleggen. Dit borgt zekerheid omdat periodiek een onafhankelijke controle bij de leverancier is uitgevoerd waarbij is vastgesteld dat deze voldoet aan de eisen voor informatiebeveiliging en privacy.

Wanneer de leverancier gecertificeerd is en daarna jaarlijks het certificaat en de bijbehorende Verklaring van Toepasselijkheid aanlevert is dit de meest eenvoudige manier om invulling te geven aan de regie op de beveiligingseisen van de ombudsman bij de leverancier. Wanneer de leverancier over een certificaat beschikt, zal de ombudsman een periodieke controle hierop uitvoeren. Zie hiervoor paragraaf 4.3.

Wanneer de leverancier beschikt over een relevant Standaard/Richtlijn 3000 Type 2 assurance-rapport dan kan deze ook gebruikt worden om regie uit te voeren. De verklaring dient daarbij wel relevant te zijn. Dat wil zeggen dat:

- het een goedkeurende verklaring is met 'een redelijke mate van zekerheid';
- de verslagperiode het huidige jaar betreft waarbij de start van de verslagperiode aansluit met het einde van de verslagperiode van voorgaande assurance-rapportage;
- de beheersingsmaatregelen omtrent informatiebeveiliging en privacy onderdeel zijn van het controleraamwerk van de leverancier;
- de processen, bedrijfsonderdelen en resources die betrokken zijn bij de dienstverlening aan de ombudsman in scope van het assurance-onderzoek zijn.

Wanneer de leverancier over een jaarlijks assurance-rapport beschikt, zal de ombudsman een periodieke controle hierop uitvoeren. Zie hiervoor paragraaf 4.3.

3.1.2 Specifiek

Wanneer de leverancier niet beschikt over de benodigde certificeringen, noch over een relevante Standaard/Richtlijn 3000 Type 2 verklaring beschikt zullen alle relevante beveiligings- en privacyeisen expliciet uitgevraagd moeten worden bij de leverancier.

Hiervoor wordt de lijst 'Informatiebeveiliging- en privacymaatregelen leveranciers' gebruikt om aan de hand van de classificatie van het betrokken middel of proces een specifiek overzicht op te stellen om met de leverancier te delen.

De basislijst uit Bijlage Informatiebeveiliging bij Leveranciersrelaties wordt aangepast met de classificatie van het systeem voor een duidelijke lijst die met de leverancier gedeeld kan worden. Zo ontstaat een overzichtelijke lijst met maatregelen met een Must of Should classificatie die door de Information Security Officer en Privacy Officer van de Leverancier ingevuld kan worden om een inschatting te geven of, en vooral hoe, er invulling gegeven wordt aan de gestelde beveiligings- en privacyeisen.

De lijst wordt via Team Informatieregie gedeeld met de leverancier zodat deze de gelegenheid heeft om deze in te vullen. De lijst moet ingevuld worden door de verantwoordelijken voor informatiebeveiliging en privacy, en middels documentatie aantoonbaar kunnen maken aan de ombudsman dat zij de vereiste maatregelen afdoende heeft geïmplementeerd.

3.1.3 Combinatie

De meeste zekerheid wordt geboden door een combinatie van beide elementen waar naast de certificeringen en/of assurance ook relevante specifieke vragen over de invulling van de beveiligingsmaatregelen worden gesteld. Het kan namelijk zijn dat de certificeringen en/of het assurance-rapport niet een volledig beeld geeft over de geïmplementeerde maatregelen bij de leverancier gedurende een sluitende periode. Ook kan het zijn dat er minor of major afwijkingen zijn gerapporteerd bij de certificeringen.

3.2 Beoordeling

De Information Security Officer beoordeelt de door de leverancier aangeleverde certificering, Verklaring van Toepasselijkheid (VvT) en/of ingevulde lijst met Beveiligingsmaatregelen. De Privacy Officer beoordeelt de door de leverancier aangeleverde certificering en/of ingevulde lijst van Privacymaatregelen. Er wordt gecontroleerd of de aangeleverde informatie volledig, correct, geldig en relevant is.

Er wordt specifiek gelet op de verwoording van hoe de leverancier de maatregel heeft ingevuld. Dit geeft vaak een goed inzicht of de leverancier de lijst heeft laten beoordelen en invullen door een medewerker met kennis van informatiebeveiliging en privacy. Een indicatie dat de lijst door een commerciële medewerker of alleen met Ja of Nee is beantwoord is voor de ombudsman reden om door te vragen.

Bij twijfel of onduidelijkheid wordt contact opgenomen met de Information Security Officer en/of Privacy Officer/Functionaris Gegevensbescherming van de leverancier

Na de beoordeling wordt een advies gegeven aan de Teamleider Informatieregie of de leverancier voldoet aan de beveiligings- en privacyeisen van de ombudsman.

De afdeling Inkoop neemt de overeengekomen beveiligings- en privacyeisen mee in de contractuele afspraken.

3.2.1 Verificatie

Het opstellen van de beveiligings- en privacyeisen en het door de leverancier laten beantwoorden of zij aan de eisen voldoen is een goede werkwijze om vooraf meer zekerheid te krijgen over het beveiligingsniveau van de uit te besteden dienst voor het aangaan van de overeenkomst. Maar het blijft een desktop-exercise. Daarom wordt een verificatie uitgevoerd wanneer de dienstverlening is gestart. Toegang tot de dienstverlening geeft de mogelijkheid om ook in de praktijk te toetsen of (een aantal van) de beveiligingseisen daadwerkelijk voldoen. Daar waar mogelijk controleert de Information Security Officer of de ingevulde lijst van de leverancier overeenkomt met de eigen bevindingen.

Wanneer de beveiligingseisen niet (volledig) blijken te voldoen wordt overleg opgestart met de leverancier om tot een volledige invulling van de beveiligingseisen te komen. Hier kan

uiteindelijk gebruik gemaakt worden van het, in de overeenkomst opgenomen, recht op het laten uitvoeren van een onafhankelijke audit.

3.2.2 Non compliant

Wanneer de leverancier niet aan de gestelde eisen voldoet zal vanuit Informatiebeveiliging en privacy geen positief advies gegeven worden om de overeenkomst af te sluiten. Op de punten waar de leverancier niet (aantoonbaar) voldoet zal een risicobeoordeling uitgevoerd worden aan de hand van de classificatie van de betrokken dienst of systeem. Alle punten waar de dienst, systeem of leverancier niet compliant is aan de eisen van de ombudsman worden als risico beoordeeld en vastgelegd in de rapportage van de risicoanalyse. De risicoanalyse wordt besproken met de (toekomstig) Systeem Eigenaar, Inkoop en eventueel de leverancier. In onderling overleg wordt afgestemd hoe de ombudsman om wil gaan met de risico's. Hierbij wordt het standaard Risicomanagement proces gevolgd zoals beschreven in het beleidsdocument Risicomanagement bij de ombudsman.

4 Tijdens de looptijd van de overeenkomst

4.1 Periodieke rapportage

Onderdeel van de standaard overeenkomst met leveranciers is dat zij periodiek rapporteren over de geleverde dienstverlening, inclusief informatiebeveiliging en privacy. Alleen wanneer de ombudsman goed op de hoogte is van de status van de beveiligingsmaatregelen bij de leverancier kan er goed invulling worden gegeven aan de verantwoordelijkheden.

De periodieke rapportage is afhankelijk van de uitbestede dienstverlening. Hieronder een overzicht van een aantal gebruikelijke rapportage-onderwerpen;

- Overzicht changes (m.b.t. Informatiebeveiliging);
- Overzicht geregistreerde (Security)incidenten, incl opvolging;
- Overzicht geregistreerde (Security)problemen, incl opvolging;
- Overzicht Patch levels betrokken systemen;
- Uitgevoerde Vulnerability scans, incl. opvolging;
- Uitgevoerde Pentests, incl. opvolging;
- Uitgevoerde autorisatiecontroles, incl. opvolging;
- Ontwikkelingen op het gebied van informatiebeveiliging bij de leverancier (Projecten, etc.).
- Overzicht van datalekken
- Wijzigingen in subverwerkers/onderleveranciers

De rapportage over informatiebeveiliging en privacy wordt gedeeld met de Information Security Officer en Privacy Officer. Onderstaande tabel wordt gehanteerd als richtlijn voor de minimale frequentie van de periodieke rapportages per classificatie.

Hoogste classificatie	Classificatie	Rapportage frequentie
BBN 1	0	Optioneel
BBN 2	1	Optioneel
BBN 2+ **	3	1 x per jaar
BBN 3	3	3 x per jaar

** geselecteerde leveranciers

4.2 Periodieke overleggen

Vanuit Team Informatieregie vindt periodiek overleg plaats met de leverancier over de dienstverlening. Een van de vaste onderwerpen op de agenda is Informatiebeveiliging. Dit kan als apart overleg of als onderdeel van een regulier overleg waar de Information Security Officer en Privacy Officer voor een deel van het overleg aanschuift. De frequentie van het overleg is afhankelijk van het belang van de uitbestede dienstverlening. Hoe hoger het belang, des te frequenter het overleg.

Onderwerpen voor het overleg:

- Bespreken Security rapportage;
- Ontwikkelingen bij leverancier met raakvlakken op informatiebeveiliging voor de ombudsman;

- Voortgang ISO 27001/NEN 7510 audit, TPM-verklaring, Standaard/Richtlijn 3000 type 2 assurance-onderzoek.

Onderstaande tabel wordt gehanteerd als richtlijn voor de minimale frequentie van de periodieke overleggen per classificatie.

Hoogste classificatie	Overleg frequentie
BBN 1	Optioneel
BBN 2	1 x per jaar
BBN 2+**	3x per jaar
BBN 3	3 x per jaar

** geselecteerde leveranciers

4.3 Periodieke controle

Naast de reguliere periodieke rapportages en overleggen met de leverancier (zie paragraaf 4.1 en 4.2) wordt ook jaarlijks een formele periodieke controle uitgevoerd. In deze periodieke controle wordt getoetst of de leverancier nog steeds aan de overeengekomen informatiebeveiligings- en privacyeisen voldoet.

De volgende controles worden jaarlijks uitgevoerd en vastgelegd in een controleverslag;

- De Information Security Officer en de Privacy Officer controleren of de lijst met de vereiste beveiligings- en privacymaatregelen bij leveranciers moet worden herzien. Indien de lijst is herzien, wordt de nieuwe herziene lijst gecommuniceerd met alle relevante leveranciers en gebruikt bij onderstaande periodieke controles;
- Controle op het jaarlijkse Standaard/Richtlijn 3000 assurancerapport. De rapportage wordt gelezen door de middeleigenaar en in geval van omissies ook de Information Security Officer en Privacy Officer. Bij het lezen van de rapportage wordt een controle uitgevoerd op een aantal elementen;
 - Bepaal het type rapport. Hierbij heeft de ombudsman de voorkeur voor een type 2 rapportage, want hierin wordt ook de werking van de controles getest, en niet enkel de opzet en het bestaan ervan, zoals in een type 1 rapportage.
 - Bepaal de rapporterende auditor. Kan worden vastgesteld dat de auditor voldoende professionele kennis, reputatie, objectiviteit en onafhankelijkheid bezit ten opzichte van de leverancier?
 - Bepaal de periode van rapportage. Hierbij heeft de ombudsman de voorkeur voor een werkingsperiode over het gehele jaar. Indien niet het hele jaar wordt afgedekt dient een zogeheten bridgeletter opgevraagd te worden bij de leverancier of zullen specifieke vragen worden gesteld over de periode waarover geen assurance is gegeven door de auditor.
 - Bepaal het bereik van de assurancerapportage. Is er sprake van onderleveranciers (subserviceorganisaties)? Het kan zijn dat de leverancier ook weer diensten heeft uitbesteed. In dat geval moet worden nagegaan of er sprake is van een zogenaamde 'carve-out' of 'inclusive'-methode. In het geval van een carve-out zijn de diensten van de onderleverancier niet meegenomen in de assurancerapportage, en dient de ombudsman een afweging te maken of deze uitbesteding relevant is voor de afgenomen diensten. Als de ombudsman de onderleverancier de onderleverancier

dermate relevant vindt voor de interne beheersing, moet een assurancerapport en/of de relevante certificeringen worden opgevraagd bij de betreffende onderleverancier.

- Bepaal of alle uitbestede diensten onderdeel zijn van de assurancerapportage. Hierbij wordt het overeengekomen contract vergeleken met de gecontroleerde diensten in de assurancerapportage.
- Bepaal of zogenaamde 'user control considerations' zijn opgenomen en of deze relevant zijn voor de ombudsman. Deze user control considerations beschrijven de interne beheersingsprocessen die de klanten van de leverancier (in dit geval de ombudsman) moeten implementeren om de doelstellingen te bereiken. Indien user control considerations relevant zijn en de ombudsman niet alle interne beheersingsprocessen heeft geïmplementeerd, dient deze opgenomen te worden in het verbeterplan.
- De middeleigenaar controleert jaarlijks of alle relevante leveranciers én onderleveranciers ISO27001 gecertificeerd zijn, het ISO 27001 certificaat is aangeleverd en of deze geldig zijn. De controle op de certificering van de onderleveranciers dient te worden uitgevoerd door de leverancier en overlegd aan de ombudsman. Tevens vindt controle plaats of de bijbehorende Verklaring van Toepasselijkheid de dienstverlening aan de ombudsman volledig afdekt en de vereiste beveiligingsmaatregelen afdoende zijn geïmplementeerd. Indien omissies zijn geconstateerd bij deze controle, wordt de Information Security Officer hiervan op de hoogte gesteld, wordt navraag gedaan bij de betreffende leverancier, wordt de impact van de omissie geëvalueerd en worden eventueel benodigde passende mitigerende maatregelen getroffen;
- De middeleigenaar of proceseigenaar controleert indien van toepassing jaarlijks van alle relevante leveranciers én onderleveranciers of zij BC5701 AVG gecertificeerd zijn, het certificaat hebben aangeleverd en of de aangeleverde BC5701 certificaten geldig zijn. De controle op de certificering van de onderleveranciers dient te worden uitgevoerd door de leverancier en overlegd aan de ombudsman. Tevens vindt controle plaats op de eventuele bijbehorende Verklaring van Toepasselijkheid de dienstverlening aan de ombudsman volledig afdekt. Indien omissies zijn geconstateerd bij deze controle, wordt de Privacy Officer op de hoogte gesteld, wordt navraag gedaan bij de betreffende leverancier, wordt de impact van de omissie geëvalueerd en worden eventueel benodigde passende mitigerende maatregelen getroffen;
- De proceseigenaar en/of de Privacy Officer controleert jaarlijks of de verwerkersovereenkomst nog volledig van toepassing is in de huidige vorm. Indien dit niet het geval is, wordt de overeenkomst herzien, opgenomen in het register en gecommuniceerd met de betreffende leverancier.

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

J Art. 5.1 lid 2 sub e

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van de eerbiediging van de persoonlijke levenssfeer van betrokkenen



nationale ombudsman

Beleid

Governance Informatiebeveiliging en Privacy

2025-2028

Document classificatie

Vertrouwelijk

Referentiedocumenten en bronnen

- Handreiking Information Security Management System (ISMS), iBD.
- Privacybeleid
- Informatiebeveiligingsbeleid

Versiebeheer

Versienummer	2.0
Eigenaar	Informatieregie \ CISO
Opgesteld door	CISO & FG
Vastgesteld door	Algemeen Directeur
Vastgesteld op datum	■ J
Laatst bijgewerkt	12-06-2025

Geschiedenis wijzigingen

Datum	Versie	Aangepast door	Beschrijving wijziging
14-07-2022	0.1	■ J	Concept (nieuwe opzet op basis van eerste versie 2021)
14-07-2022	0.2	■ J & ■ J ■ J	Uitwerking Rollen en verantwoordelijkheden
26-07-2022	0.3	■ J	Feedback
26-07-2022	0.4	■ J & ■ J ■ J	Feedback ■ J & ■ J verwerkt
01-08-2022	0.5	■ J	Tekstuele aanpassingen
27-09-2022	0.6	■ J & ■ J ■ J	Aanpassingen definitief
13-10-2022	0.7	■ J	Actualisatie document
17-11-2022	0.9	■ J	Opmerkingen ■ J & ■ J verwerkt.
18-01-2023	0.91	■ J	Opmerking n.a.v. BVO 24-11-2022 verwerkt.
20-01-2023	1.0	■ J	Vastgesteld
10-03-2025	1.1	■ J	Start met actualisatie beleid.
12-03-2025	1.2	■ J	Herzien, rol Directeur Staf / CIO uitgewerkt. Tekstuele correcties.
13-03 tm 19-03 2025	1.3	■ J, ■ J ■ J, ■ J ■ J	Review
19-03-2025	1.4	■ J, ■ J	Opmerkingen verwerkt, gereed voor CIO.
25-03-2025	1.4	■ J	Tekstuele aanpassingen nav CIO-overleg. Goedgekeurd in CIO-overleg op 24-03-2025.
12-06-2025	2.0	■ J	Vastgesteld door Alg. Dir. in DT-overleg.

Inhoud

1	INLEIDING	3
2	PDCA.....	4
2.1	PLAN	4
2.2	DO.....	4
2.3	CHECK	4
2.4	ACT.....	4
3	GOVERNANCE	5
3.1	SCOPE	5
3.2	DOEL	5
4	ROLLEN EN BELANGHEBBENDEN.....	6
4.1	ROLLEN	6
4.2	BELANGHEBBENDEN	7
5	LEIDERSCHAP EN BETROKKENHEID	8
5.1	AANSTURING: ALGEMEEN DIRECTEUR.....	8
5.2	AANSTURING: DIRECTEUR STAF	9
5.3	UITVOERING: CIO	9
5.4	UITVOERING: PROCESEIGENAAR & MIDDELEIGENAAR.....	9
5.5	CONTROLE: FG EN CISO	9
6	ROLVERANTWOORDELIJKHEDEN	10
6.1	VERANTWOORDELIJKHEIDSMATRIX	10
6.2	DETAILS VAN DE ROLLEN EN VERANTWOORDELIJKHEDEN	11
6.2.1	<i>Algemeen Directeur</i>	<i>11</i>
6.2.2	<i>Directeur Staf.....</i>	<i>11</i>
6.2.3	<i>Chief Information Officer (CIO)</i>	<i>12</i>
6.2.4	<i>Functionaris Gegevensbescherming (FG).....</i>	<i>12</i>
6.2.5	<i>Privacy Officer (PO)</i>	<i>13</i>
6.2.6	<i>Chief Information Security Officer (CISO).....</i>	<i>14</i>
6.2.7	<i>Information Security Officer (ISO).....</i>	<i>15</i>
6.2.8	<i>Proceseigenaar (Pe)</i>	<i>17</i>
6.2.9	<i>Middeleigenaar (Me)</i>	<i>18</i>
6.2.10	<i>AVG-Vertegenwoordigers</i>	<i>19</i>
7	COMMUNICATIE	20
7.1	AANPAK.....	20
7.2	COMMUNICATIEONDERWERPEN	20
7.3	COMMUNICATIEMETHODEN	21
8	PRESTATIE-EVALUATIE	23
8.1	OPERATIONELE PLANNING & CONTROL.....	23
8.2	MONITORING, METING, ANALYSE EN EVALUATIE	24
	BIJLAGE: OVERZICHT BELEIDSSTUKKEN	25

1 Inleiding

Om informatiebeveiliging en privacy binnen de ombudsman te managen maken wij gebruik van een Information Security Management System (ISMS) en een Privacy Information Management System (PIMS). Via een procesgerichte benadering borgen wij informatiebeveiliging en privacy binnen de organisatie. In dit document wordt aan beide systemen gerefereerd als de governance systematiek.

De systematiek stelt het risicobeheerproces centraal waarmee risico's adequaat kunnen worden beheerd. De systematiek is de motor van de informatiebeveiliging en privacy activiteiten en wordt onderhouden via de plan-do-check-act cyclus.

Het doel van de systematiek is het continu beoordelen of beveiligingsmaatregelen passend en effectief zijn, en of deze bijgesteld moeten worden. Het helpt de ombudsman onder andere om risico's te beheersen, passende beveiligingsmaatregelen te treffen, lering te trekken uit incidenten en daarmee de betrouwbaarheid en de kwaliteit van de informatievoorziening en bedrijfscontinuïteit te waarborgen.

Dit document beschrijft hoe die systematiek voor de ombudsman is opgezet en wie daarin welke rol heeft. Het is daarmee een omvattend document waarin verschillende aspecten die ook in andere beleidsstukken zoals het informatiebeveiligingsbeleid en het privacybeleid staan beschreven bij elkaar komen.

2 PDCA

Voor het effectueren van informatiebeveiliging en privacy wordt binnen de governance systematiek gewerkt met een verbetercyclus, de zogenaamde Plan-Do-Check-Act-cyclus (PDCA-cyclus). De 4 fasen uit de PDCA-cyclus worden hier toegelicht.

2.1 PLAN

In de PLAN-fase van de systematiek worden de informatiebeveiliging- en privacy doelstellingen voor een kalenderjaar vastgesteld. Dit wordt door de ombudsman beschreven en vastgesteld in informatiebeveiliging- en privacyjaarplan dat deel uitmaakt van het jaarplan. Deze plannen worden door de Algemeen Directeur in het DO vastgesteld.

2.2 DO

In de DO-fase wordt uitvoering gegeven aan de doelstellingen die in het jaarplan zijn opgenomen en de maatregelen die onderdeel vormen van de dagelijkse sturing van informatiebeveiliging en privacy binnen de ombudsman. Deze is voor informatiebeveiliging gestoeld op de Baseline Informatiebeveiliging Overheid (BIO) en voor de Privacy op de Algemene Verordening Gegevensbescherming (AVG). Het doel van de DO-fase is om passende informatiebeveiliging- en privacy maatregelen te selecteren voor de verschillende processen en systemen. Binnen de ombudsman is de proceseigenaar of middeleigenaar eindverantwoordelijk voor de risico's binnen zijn/ haar verantwoordingsdomein. Dit betekent dat hij/zij beslist welke controles en maatregelen getroffen moeten worden en hierover verantwoording aflegt aan het Directeurenoverleg (DO). Hierbij geldt dat het beslissen afhankelijk is van de speelruimte of het mandaat die de desbetreffende eigenaar heeft. In bepaalde gevallen kan het besluit ook door de algemeen directeur genomen worden. De CISO, FG en het DO adviseren.

2.3 CHECK

In de CHECK-fase wordt de effectiviteit en efficiëntie van de in dit document beschreven systematiek beoordeeld door middel van zelf-assessments, interne controle, (onafhankelijke) audits en bijvoorbeeld managementrapportages. De ombudsman maakt hiervoor gebruik van het systeem GRCcontrol. Binnen GRCcontrol is de hierin beschreven governance systematiek ingericht waarmee de informatiebeveiligings- en privacy prestaties en de doeltreffendheid ervan inzichtelijk worden. Voor wat betreft de toets op de BIO- en AVG-maatregelen wordt jaarlijks door de ombudsman een interne audit uitgevoerd.

2.4 ACT

Het resultaat van de CHECK-fase wordt binnen de ACT-fase gebruikt als input voor het informatiebeveiliging- en privacyjaarplan dat deel uitmaakt van het jaarplan en de privacy- en informatiebeveiligingsrapportages die elk kwartaal binnen het DO worden besproken. De ACT fase levert een beschrijving op van de stappen die nodig zijn om de concrete passende beheersmaatregelen in te voeren binnen de ombudsman op basis van de gevonden risico's of non-conformiteit. In de ACT-fase wordt dus geëvalueerd en bijgesteld op basis van de informatie uit de CHECK-fase.

3 Governance

De governance van informatiebeveiliging en privacy binnen de ombudsman gaat over de processen, de onderliggende informatiesystemen en het informatiegebruik binnen de ombudsman in de meest brede zin van het woord. De governance systematiek heeft ook betrekking op de informatie, waaronder persoonsgegevens die daarbinnen verwerkt worden. De plaats waar informatiesystemen fysiek draaien is niet van invloed. Dit betekent dat we het beleid ontwerpen, in uitvoering nemen en vervolgens regelmatig bekijken of het beleid bijstelling behoeft. De uitvoering van het informatiebeveiligingsbeleid, de 'Do fase', bestaat uit het nemen van informatiebeveiligingsmaatregelen op basis van risicoanalyses. Ook voor deze informatiebeveiligingsmaatregelen geldt een 'Plan-Do-Check-Act' cyclus in het klein. Een maatregel wordt namelijk geïmplementeerd en vervolgens wordt periodiek gecontroleerd of een maatregel werkt. Eventueel kan de maatregel bijgesteld worden of komt deze te vervallen als deze niet meer nodig is. Dit is ook het risicomanagementproces. Via een vastgesteld auditplan worden jaarlijks keuzes gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd. Deze controles kunnen dus aanleiding geven tot bijsturing in de maatregelen. Daarnaast kan het totaalpakket van eisen, maatregelen en controle aan een herijking toe zijn (evaluatie). Het goed doorlopen van deze stappen zorgt ervoor dat de ombudsman op elk moment aantoonbaar kan maken in control te zijn m.b.t tot privacy en informatiebeveiliging.

3.1 Scope

Het governancebeleid heeft betrekking op alle informatiesystemen, processen en gegevens die samenhangen met het uitvoeren van de uitvoeringstaak van de ombudsman die bestaat uit het onderzoeken, beoordelen en interveniëren m.b.t klachten die burgers hebben als zij met een overheidsorgaan te maken hebben.

3.2 Doel

Het doel van het governancebeleid is ervoor te zorgen dat ombudsman in staat is en blijft om op een veilige manier haar wettelijk vastgestelde taak uit te voeren. Hierbij is het van belang dat de ombudsman blijft voldoen aan het vastgestelde beleid waarmee potentiële en daadwerkelijke beveiligingsincidenten voorkomen kunnen worden. In het informatiebeveiligingsbeleid en het privacybeleid zijn de doelen geformuleerd. Het governancebeleid bevordert een cultuur waarin directie, managers en medewerkers zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en privacy. De rollen en verantwoordelijkheden worden hierin vastgelegd.

4 Rollen en Belanghebbenden.

In dit deel van het document worden de rollen en belanghebbenden uiteengezet die relevant zijn voor de systematiek en hun vereisten. Voor de rollen wordt een definitie beschreven en daarnaast worden de behoeften en verwachtingen van zowel de belanghebbenden als de organisatie beschreven.

4.1 Rollen

Binnen de organisatie worden er verschillende rollen op het gebied van informatiebeveiliging en privacy onderkend en zijn inclusief een definitie weergegeven in onderstaande tabel.

Rol	Definitie
Middeleigenaar (Me)	De eigenaar van een middel (met name applicaties of informatiesystemen) binnen de ombudsman en verantwoordelijk voor informatiebeveiliging en privacy in relatie tot het middel.
Proceseigenaar (Pe)	Verantwoordelijk voor de inrichting van een werkproces en daarmee ook van de informatiebeveiliging en privacy binnen het proces.
Privacy Officer (PO)	Uitvoerende rol voor privacy taken (zoals uitvoeren DPIA's, behandelen datalekken).
Information Security Officer (ISO)	Uitvoerende rol voor beveiligingsmaatregelen (zoals technische inrichting en awareness activiteiten).
Chief Information Security Officer (CISO)	Verantwoordelijk voor het toezicht op de implementatie van informatiebeveiliging, inclusief coördinatie van informatiebeveiligingsbeleid.
Functionaris Gegevensbescherming (FG)	Verantwoordelijk voor het toetsen op naleving aan de Algemeen Verordening Gegevensbescherming (AVG).
AVG-vertegenwoordigers	Aanspreekpunt voor de organisatie met betrekking tot AVG-onderwerpen en ondersteunend aan PO, FG, Pe en Me.
Chief Information Officer (CIO)	Bewaakt de samenhang in de informatievoorziening en ICT-projecten, adviseert het lijnmanagement, over het beleid ten aanzien van informatievoorziening en digitalisering.

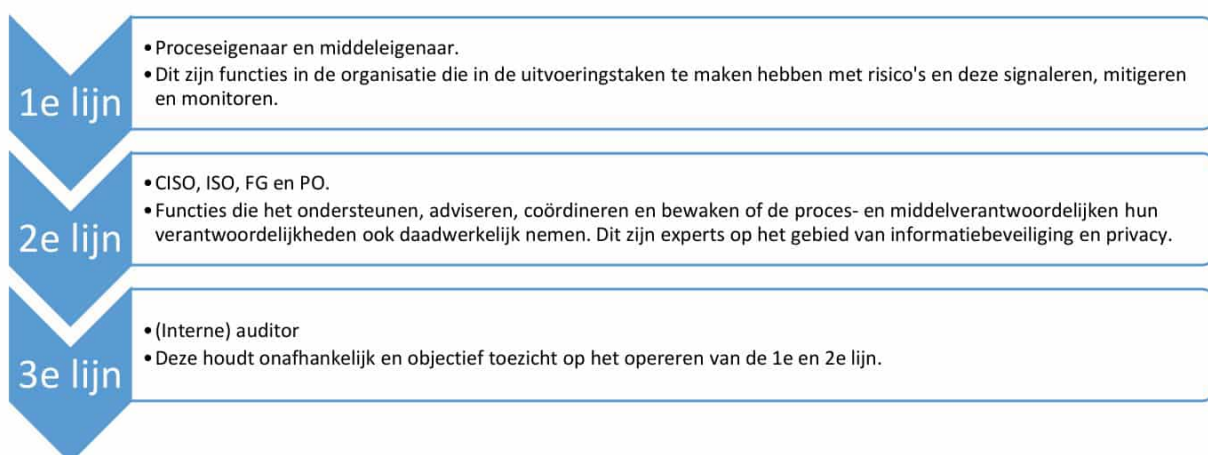
4.2 Belanghebbenden

Hieronder worden de volgende partijen gedefinieerd die relevant zijn voor de governance systematiek.

Belanghebbende	Behoefte en verwachtingen van de belanghebbende	Behoefte en verwachtingen van de organisatie
Directie	Geïnformeerd worden vanuit de (IB&P)-organisatie en betrokken bij het vaststellen van informatiebeveiligings- en privacybeleid	Strategische planning, beleid en verantwoording
Medewerkers	Bescherming van hun persoonsgegevens en het beschikbaar hebben van vereiste middelen voor de uitvoering van hun functie	Dagelijkse bedrijfsvoering
Leveranciers	Heldere opdracht en IB&P-randvoorwaarden vanuit de organisatie	In overeenstemming met SLA leveren van diensten of goederen
Regelgevende instanties	Voldoen aan de op de ombudsman van toepassing zijnde wet- en regelgeving	Naleving van de toepasselijke wet- en regelgeving en de daaraan verbonden eisen
Verzoeker	Het op een veilige en efficiënte manier behandelen en onderzoeken van verzoeken en klachten	Het zo veilig en betrouwbaar mogelijk uitvoeren van de uitvoeringstaak

5 Leiderschap en betrokkenheid

Binnen de ombudsman wordt er gewerkt met een gelaagde aanpak d.m.v. het *three lines of defence* model. Dit model beschrijft wie stuurt, bewaakt en controleert op de risico's en de implementatie van informatiebeveiliging en privacy als geheel binnen de ombudsman. Dit model zorgt ervoor dat aan de informatiebeveiligings- en privacy vereisten wordt voldaan en dat deze nauwlettend worden gecontroleerd. Hiermee wordt geborgd dat er een veilige verwerking van informatie binnen alle bedrijfsprocessen plaatsvindt. Het three lines of defence model ziet er als volgt uit:



Om het *three line of defence* model te laten functioneren is het van belang dat de rollen en verantwoordelijkheden bekend zijn. Het is van belang dat deze rollen kennis van informatiebeveiliging en privacy hebben en begrijpen wat hun rol is en waar zij verantwoordelijk voor zijn. De algemeen directeur kan deze rollen aansturen en wijzen op hun verantwoordelijkheden. Deze managementbetrokkenheid is belangrijk om informatiebeveiliging en privacy te laten landen in de organisatie. Hieronder is uiteengezet welke rollen aansturen, uitvoeren en controleren en welke verantwoordelijkheden daarbij horen.

5.1 Aansturing: Algemeen Directeur

De algemeen directeur is ervoor verantwoordelijk dat alle processen en middelen altijd onder de verantwoordelijkheid vallen van een proces- en/of middeleigenaar. Daarnaast zorgt de algemeen directeur ervoor dat de proces- en/of middeleigenaar zich verantwoordt over de beveiliging van de informatie die onder hen berust. De algemeen directeur wordt door de CISO en de FG gevraagd en ongevraagd geïnformeerd over de mate waarin informatiebeveiliging en privacy een onderdeel is van het handelen van de organisatie.

De algemeen directeur stelt het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid vast. Daarnaast is de algemeen directeur verantwoordelijk voor het (laten) uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en deze wordt hierin bijgestaan door de CISO en de FG. De algemeen directeur autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacy wordt binnen de ombudsman gezien als een integraal onderdeel van risicomanagement.

5.2 Aansturing: Directeur Staf

De Directeur Staf is verantwoordelijk voor de aansturing op de information security officer (ISO), privacy officer (PO) en de AVG-vertegenwoordigers.

5.3 Uitvoering: CIO

De CIO is voorzitter van het CIO-overleg (CIOO). Dit overleg heeft een sleutelrol in het toetsen, vertalen en beoordelen van informatiebeveiliging en privacy eisen naar de organisatie. Ze vervullen een brugfunctie tussen de algemeen directeur, directies en de proces- en middeleigenaren. Daarnaast is de CIO ook verantwoordelijk voor het initiëren van de interne audit. De ISO levert daarvoor een kalender en de CISO adviseert.

5.4 Uitvoering: Proceseigenaar & Middeleigenaar

Informatiebeveiliging en privacy vallen onder de verantwoordelijkheid van alle proces- en middeleigenaars. De proces- en middeleigenaar zijn twee aparte rollen. Dat is zo omdat middelen voor meerdere processen gebruikt worden. Als middelen slechts voor één proces gebruikt worden dan kunnen de rollen samenvallen. Als meerdere afdelingen eenzelfde proces uitvoeren, dan kan één van de leidinggevende namens alle leidinggevendenden deze rol vervullen. Afgesproken maatregelen worden dan wel door alle leidinggevendenden nageleefd. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden, die zijn verbonden aan hun rol, wel. De bedoeling is dat alle processen, informatiesystemen, data, applicaties en middelen altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn.

Proces- en middeleigenaren rapporteren aan de directeur staf (CIO) over de door hen tactisch en operationeel uitgevoerde informatiebeveiliging en privacy-activiteiten. De information security officer (ISO), privacy officer (PO) en de AVG-vertegenwoordigers ondersteunen de proces- en middeleigenaren bij de operationele uitvoering en implementatie van informatiebeveiliging en privacy.

Afstemming met proces- en middeleigenaren over de inhoudelijke aanpak vindt plaats door minimaal twee keer per jaar het onderwerp Informatiebeveiliging te bespreken in het CIO-overleg (CIOO)

5.5 Controle: FG en CISO

Het toetsen of de organisatie aan de op haar van toepassing zijnde informatiebeveiliging- en privacy vereisten voldoet valt onder de verantwoordelijkheid van de CISO en FG. De rol van zowel de CISO als FG is toetsend en ondersteunend; ze dragen zelf geen (eind) verantwoordelijkheid voor informatiebeveiliging en privacy binnen de organisatie.

6 Rolverantwoordelijkheden

In dit hoofdstuk worden de specifieke verantwoordelijkheden en bevoegdheden voor informatiebeveiliging en privacy van elk orgaan, functie en rol binnen de organisatie beschreven.

6.1 Verantwoordelijkheidsmatrix

De algemene verantwoordelijkheid voor het beheer van de verschillende onderdelen van de governance systematiek wordt weergegeven in de volgende RASCI-tabel. Dit definieert het type verantwoordelijkheid van elke rol in elk gebied van de verschillende onderdelen van de systematiek.

Verantwoordelijkheden	Algemeen Directeur	Directeur Staf / CIO	CISO	FG	PO / ISO	Proces- en Middel- eigenaar
Strategische aansturing	A	R	S	S	I	C
Security Beleid opstellen	A	R	C	C	C	C
Security Beleid goedkeuren	A	R	C	I	C	I
Privacy Beleid opstellen	A	R	C	C	C	C
Privacy Beleid goedkeuren	A	R	I	C	C	I
Plannen te nemen maatregelen	A	R	S	S	S	C
Implementeren maatregelen	A	S	S	S	S	R
Prestatie-evaluatie	A	R	C	C	S	I
Controleren op naleving privacy wet- en regelgeving	A	I	I	R	C	I
Controleren op naleving informatiebeveiliging	A	I	R	I	C	I

Tabel 1: RASCI-grafiek

R = Responsible; degenen die de activiteit uitvoeren zoals gedelegeerd door de verantwoordelijke persoon, en het kwaliteitsniveau van de output waarborgen;

A = Accountable; persoon die in het algemeen verantwoordelijk is voor de activiteit en ervoor zorgt dat deze voldoet aan het vereiste kwaliteitsniveau van de output. Kan de werkelijke activiteit (werk) delegeren aan anderen;

S = Supportive; persoon die ondersteunend is aan de R of A in het behalen van de doelstelling.

C = Consulted; degenen wier mening moet worden gevraagd (tweerichtingscommunicatie);

I = Informed; degenen die geïnformeerd moeten worden (eenrichtingscommunicatie).

6.2 Details van de rollen en verantwoordelijkheden

In deze sectie worden de specifieke verantwoordelijkheden en autoriteiten voor informatiebeveiliging van elke rol binnen de organisatiestructuur behandeld.

6.2.1 Algemeen Directeur

De algemeen directeur is eindverantwoordelijk voor informatiebeveiliging en privacy binnen de ombudsman. Deze toont leiderschap en betrokkenheid op dit gebied. Daarnaast bepaalt de algemeen directeur of een keuze in directeurenoverleg (DO) besproken moet worden, alvorens een besluit te nemen.

Verantwoordelijkheden:

- Eindverantwoordelijk voor informatiebeveiliging en privacy binnen de ombudsman en integratie hiervan binnen de bedrijfsstrategie en -governance.
- Vaststellen en goedkeuren van strategische doelstellingen op het gebied van privacy en informatiebeveiliging;
- Goedkeuren van de governance systematiek;
- Verantwoordelijk voor de jaarlijkse directiebeoordeling van informatiebeveiliging.
- Jaarlijks laten herzien en goedkeuren van het beleid en de principes van informatiebeveiliging- en privacy;
- Goedkeuring van het budget met een specifiek element dat is gereserveerd voor informatiebeveiliging en privacy;
- Het ontvangen van en adequaat handelen naar managementrapporten met betrekking tot prestatiemetingen voor informatiebeveiliging, beveiligingsincidenten, AVG, enz.;
- Eindverantwoordelijk voor de implementatie van organisatorische en technische maatregelen op processen en middelen die zorgen voor een adequate bescherming van (gevoelige) informatie.

6.2.2 Directeur Staf

De directeur staf is verantwoordelijk voor informatiebeveiliging en privacy binnen de ombudsman. Deze toont leiderschap en betrokkenheid op dit gebied. Daarnaast bepaalt de directeur staf of een keuze in het CIO en/of DO besproken moet worden, alvorens een besluit te nemen.

Verantwoordelijkheden

- Verantwoordelijk voor de implementatie van het informatiebeveiliging en privacybeleid.
- Verantwoordelijk voor uitvoering van risicomanagement op processen en middelen.
- Verantwoordelijk voor de implementatie van organisatorische en technische maatregelen op processen en middelen voor een adequate bescherming van (gevoelige) informatie.
- Verantwoordelijk voor het beheren van budgetten en middelen die nodig zijn voor informatiebeveiliging en privacy initiatieven, waaronder training van personeel of implementatie van technologieën.

- Verantwoordelijk voor coordinatie bij calamiteiten, beveiligingsincidenten voor het waarborgen van bedrijfscontinuïteit en het uitvoeren van herstelplannen, in samenwerking met de CISO.
- Verantwoordelijk voor naleving van wet- en regelgeving op operationele processen, door audits op informatiebeveiliging en privacy te initiëren en zorgen voor naleving van gegevensbeschermingsmaatregelen in de dagelijkse activiteiten.

6.2.3 Chief Information Officer (CIO)

De CIO is verantwoordelijk voor de uitvoering van informatiebeveiliging en privacy m.b.t informatie en data stromen. De CIO wordt ondersteund door de teamleider en de adviseurs binnen het team Informatieregie. Zij zullen gevraagd of ongevraagd adviseren over relevante vraagstukken.

Verantwoordelijkheden

- Verantwoordelijk voor de bewaking en controle m.b.t de opvolging van de auditbevindingen en de voorgestelde maatregelen;
- Het definiëren van controlecriteria en het bereik voor elke audit;
- Het met geplande tussenpozen laten uitvoeren van interne audits en borgen dat deze objectief en onpartijdig worden uitgevoerd;
- Het communiceren en uitdragen van het belang van het behalen van de doelstellingen en de noodzaak van voortdurende verbetering in de gehele organisatie;
- Ervoor zorgen dat de vereisten voor informatiebeveiliging en privacy worden bepaald met als doel risico's te minimaliseren en effectieve controles voor de ombudsman te handhaven;
- Het communiceren van het informatiebeveiligingsbeleid aan alle relevante en geïnteresseerde partijen;
- Risico-acceptatie door proceseigenaar en middeleigenaar te beoordelen en goed of af te keuren.
- Verantwoordelijk voor het monitoren van projecten en ervoor te zorgen dat er rekening wordt gehouden met informatiebeveiliging en privacy:
- Zorgt ervoor dat informatiebeveiliging en gegevensprivacy in de ontwerpfase worden meegenomen bij de aanschaf, wijzigingen of implementatie van nieuwe systemen:
- Plannen, opstellen, implementeren en onderhouden van een auditprogramma inclusief de frequentie, methoden, verantwoordelijkheden, planningsvereisten en rapportage;
- Definieert de auditcriteria en het toepassingsgebied voor elke audit;
- Rapporteerde de resultaten van audits aan de algemeen directeur en directie;
- Bewaart gedocumenteerde informatie als bewijs van het auditprogramma en de auditresultaten.

6.2.4 Functionaris Gegevensbescherming (FG)

De Functionaris Gegevensbescherming is een vereiste benoeming in overeenstemming met de toepasselijke wetgeving over gegevensbescherming (de Algemene Verordening Gegevensbescherming (AVG)). De FG houdt op onafhankelijke wijze toezicht op hoe de organisatie de aan hen toevertrouwde persoonsgegevens beschermt. Hieronder worden enkele hoofdtaken van de FG benoemd, maar het takenpakket is in de praktijk breder. De rol

van de FG is nader beschreven in het document rol FG.

Verantwoordelijkheden en taken

- Informeren en adviseren binnen de ombudsman. De FG informeert en adviseert de organisatie over hun verplichtingen uit hoofde van de toepasselijke wetgeving over gegevensbescherming;
- Het geven van gevraagd en ongevraagd advies aan de algemeen directeur en/of verantwoordelijk (lijn)management van de organisatie ten aanzien van privacy;
- Toezien op de naleving van de wetgeving over gegevensbescherming en het beleid van de ombudsman met betrekking tot de bescherming van persoonsgegevens. FG beoordeelt bijvoorbeeld het verplichte register van verwerkingsactiviteiten en de behandeling van AVG-verzoeken van burgers of medewerkers;
- Adviseren van de algemeen directeur over het toewijzen van verantwoordelijkheden;
- Beoordelen en goedkeuren van uitgevoerde audits en privacy impact assessments;
- Adviseren met betrekking tot data privacy impact assessments (DPIA) en het monitoren van de benodigde opvolgingsacties;
- Samenwerken met alle relevante toezichthoudende autoriteiten voor gegevensbescherming;
- Fungeren als contactpunt voor toezichthoudende autoriteiten over kwesties in verband met de verwerking van persoonsgegevens;
- Het opstellen van een actielijst voor voortdurende verbetering op en het onderhouden hiervan.

Bevoegdheden

- Melding te maken bij de toezichthoudende autoriteiten met betrekking tot gegevensbeschermingskwesties;
- De naleving van privacy binnen de gehele organisatie te controleren en te beoordelen.

6.2.5 Privacy Officer (PO)

De Privacy Officer is uitvoerend voor het opstellen, implementeren en naleven van het privacy beleid van de organisatie. De PO zorgt ervoor dat de organisatie het privacy beleid naleeft en dat de organisatie voldoet aan toepasselijke wet- en regelgeving ten aanzien van privacy (waaronder de AVG). De taken van de PO staan hieronder beschreven:

- Het opstellen van het privacy beleid;
- Het mee opstellen van het Informatiebeveiliging en privacy jaarplan;
- Het mee coördineren van de implementatie van het IB&P jaarplan;
- Het adviseren van de FG en lijnmanagement met betrekking tot privacy compliance;
- Bewustmaking en opleiding van personeel dat betrokken is bij de verwerking van persoonsgegevens;
- Het adviseren van collega's over de verwerking van persoonsgegevens;
- Het uitvoeren van pre-DPIA's;
- Het ondersteunen bij het uitvoeren van Data Protection Impact Assessments (DPIA's);
- Het bijwerken en actueel houden van het register van verwerkingsactiviteiten binnen het eigen proces;

- Het coördineren, inventariseren en registreren van datalekken, in nauwe samenwerking met de FG;
- Het beoordelen van de impact van wijzigingen in wetgeving die gevolgen hebben voor privacy;
- Het coördineren van de afhandeling van verzoeken met betrekking tot de rechten van betrokkenen, in nauwe samenwerking met de FG die de controle op de afhandeling doet;
- Adviseren over verwerkersovereenkomsten en/of samenwerkingsovereenkomsten;
- Het ontwikkelen, evalueren en beoordelen van periodieke rapportages m.b.t. privacy-compliance en privacy-risico's;
- Het adviseren over privacy en de uitgangspunten van privacy-by-design bij de start en tijdens de uitvoering van nieuwe projecten;
- Het verzorgen met de FG van compliance-rapportages en risico-rapportages aan de directie en portefeuillehouder(s).

6.2.6 Chief Information Security Officer (CISO)

De rol van de CISO is ondersteunend maar tegelijkertijd ook sturend. De CISO geeft namelijk gevraagd en ongevraagd advies op alle aangelegenheden die betrekking hebben op informatiebeveiliging. Dit kan hij alleen doen of in samenspraak met de Functionaris Gegevensbescherming (FG) of Chief Information Officer (CIO). De taken en verantwoordelijkheden zijn onderverdeeld in de volgende gebieden:

Beleid en coördinatie

- Het (laten) opstellen en actualiseren van het informatiebeveiligingsbeleid (langere termijn);
- Het toetsen informatiebeveiligingsplannen voor afdelingen of deelgebieden (jaarplannen);
- Het coördineren van de werkzaamheden van personen, afdelingen en instanties die betrokken zijn bij de uitvoering van het informatiebeveiligingsbeleid;
- Het organiseren van en deelnemen aan een coördinerend overleg met betrekking tot informatiebeveiliging;
- Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging;
- De organisatie vertegenwoordigen in externe gremia;
- Het aanspreekpunt zijn voor informatiebeveiligingsincidenten en vragen. Wanneer zich een groot incident voordoet roept de CISO het CERT-team bijeen om de voorbereide stappen uit te voeren om het incident zo goed en snel mogelijk op te lossen;

Controle en registratie

- Het toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid;
- Het opstellen van een controleplan;
- Het desgevraagd initiëren van risicoanalyses en interne audits;

- Het monitoren van de opvolging van maatregelen die uit een risicoanalyse voortvloeien;
- Het monitoren van de aanwezige beveiligingsmaatregelen;
- Het monitoren van beveiligingsincidenten, evenals het aansturen van de afhandeling van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten;
- Optreden als informatiebeveiligingsadviseur bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICT-Infrastructuur.

Communicatie en voorlichting

- Het verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van informatiebeveiliging;
- Het stimuleren van het beveiligingsbewustzijn en het opstellen, uitvoeren en onderhouden van een communicatieplan;
- Het onderhouden van externe en interne contacten op alle niveaus binnen dit resultaatgebied.

Advies en rapportage

- Het geven van gevraagd en ongevraagd advies aan de algemeen directeur en/of verantwoordelijk (lijn)management van de organisatie ten aanzien van informatiebeveiliging;
- Het rapporteren aan de algemeen directeur over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en resultaten van controles;
- Het optreden als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen organisatorische eenheden.

6.2.7 Information Security Officer (ISO)

De Information Security Officer (ISO) is geen vaste rol binnen de ombudsman. De uitvoering van de genoemde taken wordt ingevuld door externe partners of leveranciers. Dit zal inhoudelijk zijn op het gebied van het verbeteren van informatiebeveiligingsbeleid en risicomanagement. Daarnaast kan de ISO gevraagd worden om het lijnmanagement te ondersteunen en adviseren, toezien op naleving en realisatie van het beleid.

De ISO werkt op organisatie breed niveau waardoor het essentieel is om in nauw contact te staan met de CISO, lijnmanagers, projectmanagers, leveranciers en auditors. Om op de hoogte te blijven van de nieuwste technologische ontwikkelingen is contact met leveranciers (beurzen, lidmaatschap, gebruikersgroepen van bepaalde producten) ook van groot belang. De taken en verantwoordelijkheden zijn onderverdeeld in de volgende gebieden:

Beleid en coördinatie

- Het ondersteunen van de CIO bij het opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid;

- Adviseren van het (lijn)management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden en bij de implementatie van deze plannen;
- Het ondersteunen van de werkzaamheden van personen, afdelingen en instanties die betrokken zijn bij de uitvoering van het informatiebeveiligingsbeleid;
- Het organiseren van en deelnemen aan een coördinerend overleg met betrekking tot informatiebeveiliging;
- Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging.

Controle en registratie

- Het toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid;
- Het opstellen van een controleplan, evenals het in de vorm van de ISO leveren van ondersteuning bij het uitvoeren van de daarin gedefinieerde taken;
- Het bijdragen aan een controleplan, evenals het in de vorm van de ISO leveren van ondersteuning bij het uitvoeren van de daarin gedefinieerde taken;
- Het uitvoeren van dataclassificaties en risicoanalyses. De bevindingen worden in overeenstemming met de risicomanagement procedure vastgelegd en opgevolgd. Hierbij ondersteun je de lijnorganisatie bij het beheersen en mitigeren van de risico's;
- Het uitvoeren van, en bijdragen aan de uitvoering van maatregelen die uit een risicoanalyse voortvloeien;
- Het verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen;
- Het opzetten of initiëren van een registratie voor beveiligingsincidenten, evenals het ondersteunen tijdens de afhandeling van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten;
- Het initiëren en begeleiden van penetratietests op onze (informatie)systemen en infrastructuur om aantoonbaar te maken dat ze aan onze beveiligingseisen voldoen.

Communicatie en voorlichting

- Het stimuleren van het beveiligingsbewustzijn en het opstellen, uitvoeren en onderhouden van een communicatieplan;
- Het onderhouden van externe en interne contacten op alle niveaus binnen dit resultaatgebied;
- Ontwerpen van beveiligingsmaatregelen op basis van risicoafwegingen, deze afstemmen met de lijnorganisatie en hen adviseren bij de implementatie daarvan.

Advies en rapportage

- Het bieden van ondersteuning bij beveiligingsprojecten;
- Het afstemmen van informatiebeveiliging met lopende projecten binnen de organisatie.
- Het uitwerken van beveiligingsplannen ten aanzien van de maatregelen, evenals het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen;
- Desgevraagd een ondersteunende rol vervullen tijdens risicoanalyses die door proceseigenaren en systeemeigenaren worden uitgevoerd;

- Verwerken van onafhankelijke controles en audit om deze bevindingen in de organisatie te beleggen en tot een goede oplossing te begeleiden.

6.2.8 Proceseigenaar (Pe)

De proceseigenaar beslist over de inrichting en het verloop van een proces en is verantwoordelijk dat dit proces blijft voldoen aan het beleid van de ombudsman, de 'klant'-verwachtingen en organisatiedoelstellingen. De proceseigenaar bepaalt dus de hoe het proces gaat verlopen en wat de resultaten van het proces moeten zijn. Om het proces in te richten dient de proceseigenaar het proces te analyseren en risico's in kaart te brengen. Voor deze risico's moeten passende maatregelen worden getroffen door de proceseigenaar. De proceseigenaar is daarnaast ook verantwoordelijk voor de gegevens die binnen hun proces worden gebruikt, waarbij het niet uitmaakt waar de gegevens van afkomstig zijn en/of waar ze naartoe gaan. De verantwoordelijkheid van de proceseigenaar hiervoor begint zodra deze het proces binnen zijn gekomen en eindigt zodra ze het proces verlaten.

Verantwoordelijkheden

- Is eindverantwoordelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid binnen het proces en legt hier periodiek verantwoording over af aan de algemeen directeur;
- Beslist over wie toegang krijgt tot gegevens, en dus tot de autorisatie van medewerkers voor rollen in de applicaties (toegangsbeveiligingsbeleid);
- Richt het proces in en toetst deze aan beleid, "klant"verwachtingen en organisatiedoelstellingen;
- Beslist over wijzigingen op basis van het wijzigingsbeheerbeleid in processen (inclusief hulpmiddelen en werkprocessen) en de vast te leggen gegevens;
- Is verantwoordelijk voor de risicobehandeling m.b.t de risico binnen het proces op basis van het risicomanagementbeleid en is ervoor verantwoordelijk dat de adequate maatregelen worden getroffen om de risico's te beheersen;
- Verantwoordelijk voor de rapportages;
- Draagt het belang uit van het goed volgen van de afgesproken werkprocessen;
- Is verantwoordelijk voor privacy- en informatiebeveiligingawareness betreffende het eigen proces.
- Zorgt ervoor dat de documentatie over het proces actueel is;
- Communiceert over de ontwikkelingen rond het werkproces aan de algemeen directeur.
- Is verantwoordelijk voor het laten opstellen van beleid m.b.t de kwaliteit van de gegevens;
- Is verantwoordelijk om te voldoen aan de AVG vereisten die op hun proces van betrekking zijn;
- Is verantwoordelijk om te voldoen aan de BIO vereisten die op hun proces van betrekking zijn;
- Bepaalt het basisbeveiligingsniveau van het proces (op basis van het BIO kader);
- Dagelijkse implementatie van het informatiebeveiligingsbeleid;
- Zorgt voor passende technische, fysieke en procedurele controles die in overeenstemming zijn met het beleid en dat deze correct worden toegepast en

gebruikt door alle werknemers. Zij moeten maatregelen nemen om ervoor te zorgen dat werknemers binnen het proces:

- worden geïnformeerd over hun verplichtingen om te voldoen aan relevante bedrijfsbeleidsverklaringen door middel van passende bewustmakings-, trainings- en opleidingsactiviteiten.
 - voldoen aan de beleidsverklaringen en de bijbehorende controles actief ondersteunen; en;
 - worden gecontroleerd om hun naleving van de beleidsverklaringen en de correcte werking van de bijbehorende controles te beoordelen en waar nodig aan hun verplichtingen worden herinnerd.
- Verantwoordelijk voor het geven van richting, middelen, ondersteuning die nodig zijn om ervoor te zorgen dat informatiemiddelen op passende wijze worden beschermd binnen hun verantwoordelijkheidsgebied;
 - Het informeren van de CISO, FG over feitelijke of vermoedelijke beleidsschendingen (informatiebeveiligingsincidenten) die van invloed zijn op hun proces;
 - Het evalueren van de naleving van het beleid en de interne audits; en de opvolging van auditbevindingen.

6.2.9 Middeleigenaar (Me)

De middeleigenaar is verantwoordelijk voor het juist functioneren van de systemen, data, applicaties en middelen waar de ombudsman gebruik van maakt. De middeleigenaar is verantwoordelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van de middelen die onder hun verantwoordelijkheid vallen en ervoor te zorgen dat ze blijft voldoen aan het beleid, de security baseline, de klantverwachtingen en bedrijfsdoelstellingen.

De middeleigenaar gaat over de inrichting en het mogelijke ontwerp van het middel en is verantwoordelijk voor de resultaten van de werking van het middel.

Verantwoordelijkheden

- Richt het middel in en toetst deze aan beleid, de security baseline, AVG, doelgroep verwachtingen en bedrijfsdoelstellingen;
- Richt de toegangsrechten tot middelen en gegevens in op basis van de autorisatietabel (die de proceseigenaar heeft opgesteld);
- Rapporteert periodiek aan de proceseigenaar over wie toegang heeft of de beschikking heeft over een middel;
- Is verantwoordelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van het middel;
- Beslist over functionele wijzigingen m.b.t het middel;
- Stemt met de proceseigenaar niet-functionele wijzigingen af;
- Budgethouder voor onderhouds- en wijzigingsbudget;
- Draagt het belang uit van het juiste gebruik van het middel;
- Zorgt ervoor dat de documentatie van het middel up-to-date is;
- Communiceert over de ontwikkelingen rondom het middel;
- Inventariseren van wensen en eisen van proceseigenaar, CISO en FG;
- Verantwoordelijk voor de aanschaf, vervanging en vernietiging van de benodigde middelen;
- Plan opstellen voorafgaand aan de implementatie voor het onderhoud en ondersteuning van middelen;

- Tekent voor elke aanpassing die in productie wordt genomen;
- Sluit een SLA af met de beheerorganisatie of leverancier over o.a. beschikbaarheid van middelen.

6.2.10 AVG-Vertegenwoordigers

De AVG-vertegenwoordiger brengt het privacy beleid - in samenwerking met het management - onder de aandacht van de medewerkers van de eigen directie, met als doel om het privacy bewustzijn te vergroten binnen de ombudsman en daarnaast te ondersteunen met het borgen van het privacy beleid.

Binnen elke directie (organisatieonderdeel) van de ombudsman wordt minimaal één AVG-vertegenwoordiger benoemd. De AVG-vertegenwoordigers ontvangen periodiek (interne) scholingsactiviteiten om hun kennisniveau op peil te houden. De AVG-vertegenwoordiger heeft de volgende taken:

- Fungeren als 'adviesloket' bij vragen binnen de eigen dienst over de AVG. De AVG-vertegenwoordiger fungeert als eerste aanspreekpunt binnen de eigen dienst voor vragen over de AVG.
- Inventariseren, beoordelen, bijhouden en melden van verwerkingen persoonsgegevens in het AVG-register.
- Fungeren als aanspreekpunt voor de Privacy Officer bij incidenten (waaronder datalekken) en privacy verzoeken.
- Zorgen dat de AVG blijvend onder de aandacht is van de medewerkers van de eigen dienst en draagt zo bij aan het privacy bewustzijn van de medewerkers van de ombudsman.
- Deelname aan het maandelijks AVG-overleg en vervolgens relevante onderwerpen binnen de eigen dienst onder de aandacht brengen.

7 Communicatie

De ombudsman beschikt over een governance- en controle raamwerk dat de organisatie gebruikt om haar informatiemiddelen te beschermen en de vastgestelde risico te verminderen. Het is belangrijk dat iedereen die betrokken is bij het raamwerk begrijpt wat hun rol is en hoe de activiteiten die ze uitvoeren bijdragen aan het voldoen aan de bedrijfs- en informatiebeveiliging en privacy vereisten en de algemene doelstellingen van de organisatie.

Het opzetten en voortdurend onderhouden van bewustzijn en competentie op het gebied van informatiebeveiliging is een belangrijk proces binnen de systematiek, omdat het ten grondslag ligt aan veel van de andere processen die in gebruik zijn.

Het creëren en onderhouden van een effectieve relatie met proceseigenaar en systeemeigenaren, gebruikers en andere geïnteresseerden zal ervoor zorgen dat informatiebeveiliging- en privacy controles worden geïmplementeerd op de manier die bij de ombudsman past, waardoor de impact op de bedrijfsvoering zoveel mogelijk zal worden beperkt.

In dit hoofdstuk wordt uiteengezet hoe belanghebbenden binnen en buiten de ombudsman worden geïnformeerd over informatiebeveiliging en privacy. Hierin wordt aangegeven wie de belanghebbenden zijn en hoe een effectief communicatiekanaal tot stand zal komen.

7.1 Aanpak

De algemene aanpak om te zorgen voor effectieve betrokkenheid en communicatie binnen ombudsman is als volgt:

1. Identificeer de belanghebbenden.
2. Definieer de juiste communicatieonderwerpen voor elke belanghebbende partij.
3. Spreek de meest geschikte methoden van betrokkenheid en communicatie af.
4. Uitvoering van het programma.
5. Feedback krijgen en reageren op het succes van de communicatie, via input voor het continu verbeterplan.

Deze stappen worden afzonderlijk behandeld in de volgende hoofdstukken.

7.2 Communicatieonderwerpen

Het communicatieprogramma is bedoeld om de belangrijkste informatie te communiceren op de volgende hoofdgebieden:

- De bedrijfsomgeving waarop de systematiek betrekking heeft, inclusief belangrijke veranderingen wanneer deze zich voordoen.
- Het algemene kader van de systematiek inclusief de visie, het beleid, de plannen en de doelstellingen die moeten worden bereikt.
- Hoe de geldende informatiebeveiligings- en privacy maatregelen zich verhouden tot de behoeften van de ombudsman, zowel nu als in de toekomst.
- Hoe de systematiek bedoeld is om de privacy- en informatiebeveiligingsvereisten vast te leggen en hieraan te voldoen.

- De wettelijke, reglementaire en contractuele vereisten en beperkingen waarbinnen de systematiek moet werken.
- Updates over hoe de plannen vorderen om de gedefinieerde doelstellingen van de systematiek te bereiken.
- Bewustzijn van informatiebeveiligingskwesties en -risico's en onze aanpak ervan.

Het detailniveau dat op de bovengenoemde gebieden vereist is, zal per belanghebbende partij verschillen.

7.3 Communicatiemethoden

Binnen de ombudsman zijn een aantal gevestigde communicatiemethoden en -momenten aanwezig en deze zullen waar mogelijk worden gebruikt. Deze omvatten:

- CIO-overleg;
- Directeurenoverleg;
- Privacy en securityteam overleggen;
- Regelmatige teamvergaderingen en briefings;
- Berichtgeving op intranet;
- Presentaties;
- E-learning / Webinars;
- Ad-Hoc evenementen;

In nader te bepalen gevallen zullen aanvullende methoden worden ingevoerd, hetzij tijdelijk, hetzij permanent, ter aanvulling van de al beschikbare methoden. In de volgende tabel wordt een uitsplitsing gegeven van de wijze waarop de nodige informatie aan de betrokken belanghebbenden zal worden meegedeeld.

BELANGHEBBENDE	ONDERWERP VAN COMMUNICATIE	METHODE / MOMENT	FREQUENTIE
Algemeen Directeur	1. Informatiebeveiliging en privacy strategie/jaarplan 2. Risicomanagement	1. Presentatie 2. Schriftelijk	Jaarlijks
Directie	1. Voortgangsrapportage	1. Schriftelijk	Kwartaal
CIO	1. Risicomanagement (hoog over) 2. Projecten en activiteiten 3. Voortgangsrapportage 4. Voortgang privacy en informatiebeveiliging implementatie	1. Presentatie 2. Schriftelijk 3. Vergadering	Maandelijks
Proces-verantwoordelijken/ systeemeigenaren	1. Te implementeren maatregelen 2. Uit te voeren risicoanalyses, BIA of DPIA's 3. Awareness activiteiten 4. Incident opvolging	1. Vergadering 2. Teammeetings 3. 1 op 1	Ad-hoc

Medewerkers	1. Mededeling van het informatiebeveiligingsbeleid en privacybeleid 2. Ad-hoc herinneringen bij belangrijke gebeurtenissen, bijv. incidenten 3. Waarschuwingen en bewustzijn	1. Bewustwordings-trainingen	Jaarlijks (frequentie wordt verhoogd in geval van nood)
Verzoekers/ derden	1. Communicatie van informatiebeveiliging en privacy vereisten 2. Suggesties voor verbetering.	1. Privacyverklaring 2. Responsible disclosure	Website en tijdens contact momenten.
Leveranciers	1. Privacy en informatiebeveiligingsvereisten 2. Contractuele vereisten 3. Suggesties voor verbetering	1. Leveranciersbijeenkomsten 2. Contracten	Alvorens het contract wordt ondertekend.

Effectieve communicatie met belanghebbende partijen is de sleutel tot het succes van de implementatie van de governance systematiek binnen ombudsman. De communicatiemethoden in dit document moeten ertoe bijdragen dat alle betrokkenen goed op de hoogte blijven van informatiebeveiligingskwesties en de mogelijkheid hebben om feedback te geven over zowel de gebruikte kanalen als de inhoud ervan.

8 Prestatie-evaluatie

Een effectieve governance systematiek helpt de ombudsman een goede mate van bescherming te bieden tegen risico's van bedreigingen voor de beschikbaarheid, integriteit en vertrouwelijkheid van zijn informatiemiddelen. Dit vereist dat de ombudsman de informatiebeveiliging- en privacy prestaties en de effectiviteit van de systematiek evalueert, zodat de organisatie in control is en daar waar nodig kan bijsturen. Binnen de in hoofdstuk 2 genoemde PDCA-cyclus omvat dit hoofdstuk de Check en Act fase. Dit hoofdstuk beschrijft de aanpak die de ombudsman volgt bij het monitoren en meten van de systematiek en hoe de resultaten worden geïnterpreteerd om eventuele vereiste acties voor verbetering uit te zetten.

8.1 Operationele Planning & Control

In dit hoofdstuk wordt beschreven op welke wijze de ombudsman beoordeelt of de getroffen maatregelen nog in lijn zijn met de aanwezige risico's. Om dit te bewerkstellingen zal de ombudsman de volgende activiteiten uitvoeren:

- Willekeurig uitvoeren van controles op de geïmplementeerde maatregelen;
- Uitvoeren van audits (intern en extern);
- Kwetsbaarheids- en risicobeoordelingen uit te voeren;
- Uitvoeren van pentesten;
- Uitvoeren programma informatiebeveiliging en privacy bewustzijn.

Deze activiteiten worden uitgevoerd met als doel om te toetsen of de genomen maatregelen adequaat zijn in relatie tot de aanwezige risico's en het steeds veranderende informatiebeveiliging en privacy landschap. De ombudsman borgt hiermee dat het continue op de hoogte is van de aanwezig risico's en de mogelijke impact die deze zouden kunnen vormen.

De CIO zorgt voor de aansturing van dit onderdeel. Dit houdt in het (laten) plannen, opstellen, implementeren en onderhouden van een auditprogramma inclusief de frequentie, methoden, verantwoordelijkheden, planningsvereisten en rapportage en is daarnaast verantwoordelijk voor het definiëren van de auditcriteria en het toepassingsgebied voor elke audit.

Door het uitvoeren van audits, kwetsbaarheids- en risicobeoordelingen en pentesten wordt inzicht gecreëerd in de bestaande risico's. Op basis van de resultaten kan de ombudsman concrete maatregelen nemen om de aanwezige risico's af te dekken en is ze in staat om de genomen maatregelen te controleren op effectiviteit.

Deze activiteiten en de resultaten hiervan worden opgenomen in de GRC-tool. De GRC-tool helpt bij het signaleren van uit te voeren controles en bij het verantwoorden van de prestaties binnen de ombudsman en naar externe toetsende instanties.

8.2 Monitoring, meting, analyse en evaluatie

Om te borgen dat de ombudsman continue op de hoogte is van de aanwezige risico's is er een monitoringssystematiek opgesteld. Deze systematiek borgt dat op basis van de belangrijkste informatiebronnen periodiek wordt gerapporteerd.

Bewaakt gebied	Metriek	Inzamelings-methode	Verzamel-frequentie	Verantwoordelijk	Bron/uitkomst
Beveiligingsincidenten	Aantal beveiligingsincidenten, naar ernst	Via incident managementproces	Continu	CISO	Topdesk
Risico 's	Aantal risico's, per prioriteit	Risicomanagementbeleid en het Risicoregister in GRC	Kwartaal	CISO/ FG	Risicoregister in GRC
Bedreigingen	Aantal gemelde nieuwe bedreigingen	Risicomanagementbeleid en het Risicoregister in GRC	Continu	CISO/ FG	Risicoregister in GRC
Kwetsbaarheden	Aantal nieuwe kwetsbaarheden gedetecteerd	Als gevolg van regelmatige penetratietests	Doorlopend	ISO (uitvoering door externen)	Pentest rapporten
Informatiemiddelen	Aantal informatieactiva, naar classificatie	Interviews met de CISO/ FG	Continu	Proces-verantwoordelijken/ system eigenaren	Middelen overzicht in GRC
Directiebeoordeling	Doelstellingen vs. bereikte doelstellingen genoemd in het jaarplan	Rapportage door FG en CISO opgesteld	Jaarlijks	CISO/ FG	Notulen van de vergadering
Awareness	Aantal uitgevoerde awareness activiteiten	Proces en systeemeigenaren houden dit bij en leveren input	Kwartaal	Proces en systeemeigenaren	Rapportage aan CISO/ FG
Non-conformiteit	Aantal geïdentificeerde non-conformiteit m.b.t BIO en AVG.	Controleverslagen	Interne audit	CIO voor het laten uitvoeren van de interne audit.	Auditrapport in GRC

Bijlage: Overzicht beleidsstukken

De governance systematiek beschrijft op welke wijze de organisatie op strategisch met informatiebeveiliging en privacy omgaat. De tactische en operationele uitvoering van dit beleid is geregeld in de verschillende beleidstukken. De binnen de ombudsman gebruikte beleidsstukken zijn in onderstaande tabel opgenomen.

Beleidsstuk	BIO /AVG	Goedkeuring door	Verantwoordelijke
Informatiebeveiligingsbeleid	BIO	Algemeen Directeur	Directeur Staf (CIO)
Risicomanagement	BIO	Algemeen Directeur	Directeur Staf (CIO)
Incidentmanagement	BIO	Algemeen Directeur	Directeur Staf (CIO)
HR Beleid	BIO	Algemeen Directeur	Directeur Staf (CIO)
HR Screeningsbeleid	BIO	Algemeen Directeur	Directeur Staf (CIO)
Toegangsbeveiligingsbeleid	BIO	Algemeen Directeur	Directeur Staf (CIO)
Wachtwoordbeleid	BIO	Algemeen Directeur	Directeur Staf (CIO)
Wijzigingsbeheer	BIO	Algemeen Directeur	Directeur Staf (CIO)
Informatieclassificatie	BIO	Algemeen Directeur	Directeur Staf (CIO)
Aanvaardbaar gebruik	BIO	Algemeen Directeur	Directeur Staf (CIO)
Back-up beleid	BIO	Algemeen Directeur	Directeur Staf (CIO)
Bedrijfscontinuïteitsbeheer	BIO	Algemeen Directeur	Directeur Staf (CIO)
Beveiligd ontwikkelen	BIO	Algemeen Directeur	Directeur Staf (CIO)
Draagbare apparatuur	BIO	Algemeen Directeur	Directeur Staf (CIO)
Intern auditprocedure	BIO	Algemeen Directeur	Directeur Staf (CIO)
Telewerken	BIO	Algemeen Directeur	Directeur Staf (CIO)
Kwetsbaarheden & Patchmanagement	BIO	Algemeen Directeur	Directeur Staf (CIO)
Leveranciersmanagement	BIO	Algemeen Directeur	Directeur Staf (CIO)
Cryptografisch beleid	BIO	Algemeen Directeur	Directeur Staf (CIO)
Fysieke beveiliging	BIO	Algemeen Directeur	Directeur Staf (CIO)
Malwarebeleid	BIO	Algemeen Directeur	Directeur Staf (CIO)
Communicatiebeveiliging	BIO	Algemeen Directeur	Directeur Staf (CIO)
Awareness (Wallpapers, e-learning)	BIO & AVG	Algemeen Directeur	Directeur Staf (CIO)
Governance IB&P	BIO & AVG	Algemeen Directeur	Directeur Staf (CIO)
AVG verzoeken	AVG	Algemeen Directeur	Directeur Staf (CIO)
Privacy statement	AVG	Algemeen Directeur	Directeur Staf (CIO)
Privacy beleid	AVG	Algemeen Directeur	Directeur Staf (CIO)
Protocol datalekken	AVG	Algemeen Directeur	Directeur Staf (CIO)
Rol beschrijving FG	AVG	Algemeen Directeur	Directeur Staf (CIO)
Gebruik persoonsgegevens	AVG	Algemeen Directeur	Directeur Staf (CIO)
Informatieblad AVG	AVG	Algemeen Directeur	Directeur Staf (CIO)
DPIA procedure	AVG	Algemeen Directeur	Directeur Staf (CIO)
Privacy by design	AVG	Algemeen Directeur	Directeur Staf (CIO)

Informatieblad AVG voor medewerkers

Dit informatieblad is van toepassing op medewerkers en externen die voor de Nationale ombudsman, Veteranenombudsman en/of Kinderombudsman (hierna: ombudsman) werken (hierna medewerkers).

Doel van dit informatieblad is om medewerkers te informeren over de wijze waarop de ombudsman met persoonsgegevens van medewerkers omgaat en hoe medewerkers hun AVG rechten kunnen uitoefenen.

Heb je na het lezen van dit informatieblad nog vragen, neem dan contact op met de [functionaris gegevensbescherming](#) of één van de [AVG vertegenwoordigers](#).

Gebruik van persoonsgegevens

De ombudsman gaat zorgvuldig om met persoonsgegevens en houdt zich aan de eisen die de AVG stelt. De ombudsman verwerkt persoonsgegevens van medewerkers uitsluitend voor de doeleinden waarvoor de persoonsgegevens zijn verstrekt. Persoonsgegevens van medewerkers worden voor verschillende doeleinden verwerkt. Denk bijvoorbeeld aan het verwerken van persoonsgegevens voor:

- de uitvoering van het desbetreffende dienstverband (zoals uitvoering arbeidsvoorwaarden, beoordeling functioneren, registratie verzuim etc);
- aan het dienstverband gerelateerde doeleinden (zoals opleiding, boeken dienstreizen, monitoren integriteit/nevenfuncties);
- het voldoen aan wet- en regelgeving op het gebied van sociale lasten (premies, volksverzekeringen en pensioen) en op het gebied van heffingen (belasting);
- het uniek kunnen identificeren van een medewerker m.b.v. het RIN nummer;
- interne controle (zoals op gebruik OV kaart) of het uitvoeren van onderzoek (zoals het medewerkersonderzoek);
- het kunnen uitvoeren van het werk (zoals de dossiervorming en registratie in Verseon en regelen toegang tot systemen/accounts);
- het behandelen van klachten over medewerkers;
- het reserveren van facilitaire diensten (zoals een vergaderzaal), de uitgifte van laptop en telefoon en het kunnen gebruiken van de kopieerapparaten;
- informatieverstrekking (via bijvoorbeeld website, NoHow en nieuwsbrief Jouw Nieuws);
- beveiliging (registratie beveiligingsincidenten, bedrijfshulpverlening, toegangscontrole, cameratoezicht).

Ontvangers

De ombudsman verstrekt persoonsgegevens van medewerkers aan andere organisaties. Als dit gebeurt, gebeurt dit zorgvuldig en alleen voor zover dit noodzakelijk is. Denk bijvoorbeeld aan het verstrekken van persoonsgegevens aan de Arbodienst of aan een opleider voor cursussen.

Verwerkers

Wanneer de ombudsman persoonsgegevens van medewerkers deelt met leveranciers, dan sluit de ombudsman met deze leveranciers een verwerkersovereenkomst. Daarin staat onder meer dat de verstrekte persoonsgegevens alleen voor het overeengekomen doel mogen worden gebruikt, dat deze adequaat beschermd moeten zijn en dat de leverancier de gegevens moet vernietigen wanneer deze niet meer nodig zijn.

Bewaartermijn

Persoonsgegevens worden niet langer bewaard of verder verwerkt dan noodzakelijk voor de doeleinden waarvoor ze zijn verzameld. De bewaartermijn verschilt per (categorie) persoonsgegevens.

De bewaartermijn voor personeelsdocumenten ligt vast in het [basisselektiedocument P-dossier is Mens-en-werk](#) (verkort BSD P-Direkt).

Beveiliging van persoonsgegevens

Wij hebben passende technische en organisatorische maatregelen getroffen om jouw persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking, waaronder maar niet beperkt tot beveiliging door wachtwoorden, beveiligde dataopslag, een aparte afgesloten ruimte om personeelsdocumenten te bewaren en een alarm om het pand te beveiligen.

Verwerkingenregister

In het [verwerkingenregister](#) van de ombudsman staan alle verwerkingen waarin persoonsgegevens van medewerkers worden verwerkt. Per verwerking kun je hierin onder meer vinden:

Wie verantwoordelijk is voor de verwerking

Wie de gegevens ten behoeve van de verwerkingsverantwoordelijke verwerkt (de verwerker)

Aan welke andere organisaties de gegevens worden verstrekt (de ontvangers)

Met welk doel de persoonsgegevens worden verwerkt

Van wie (categorieën betrokkenen) gegevens worden verwerkt, welke gegevens dit zijn en van wie ze afkomstig zijn (de bron).

Welke systeem/applicatie voor de verwerking wordt gebruikt

De maatregelen die zijn genomen om de persoonsgegevens te beschermen

Heb je vragen over het verwerkingenregister neem dan contact op met de functionaris gegevensbescherming of één van de [AVG vertegenwoordigers](#).

Heb je vragen over het verwerkingenregister neem dan contact op met de functionaris gegevensbescherming of één van de AVG vertegenwoordigers.

Rechten

Medewerkers kunnen een beroep doen op de rechten die de AVG aan betrokkenen biedt. Onderstaande tabel laat zien om welke rechten het gaat.

Recht	Artikel	Omschrijving
Recht op inzage	Artikel 15 AVG	Het recht om te vragen welke persoonsgegevens de organisatie van jou heeft en om deze persoonsgegevens in te zien.
Recht op rectificatie	Artikel 16 AVG	Het recht om onjuiste persoonsgegevens te laten wijzigen of om persoonsgegevens aan te vullen.
Recht op beperking van de verwerking	Artikel 18 AVG	Het recht om minder gegevens te laten verwerken. Onder de AVG geldt dit recht alleen in situaties die voldoen aan de in de AVG genoemde criteria.
Recht met betrekking tot geautomatiseerde besluitvorming en profilering	Artikel 22 AVG	Geautomatiseerde besluitvorming komt bij de ombudsman niet voor.
Recht van bezwaar	Artikel 21 AVG	Als medewerker heb je het recht om bezwaar aan te tekenen tegen de verwerking van jouw persoonsgegevens.
Recht op dataportabiliteit	Artikel 20 AVG	Dit recht is gericht op commerciële diensten en daarom voor medewerkers van de ombudsman minder relevant.
Recht op vergetelheid	Artikel 17 AVG	Dit recht houdt in dat organisaties in een aantal gevallen jouw persoonsgegevens moeten wissen als jij daarom vraagt. Het recht op vergetelheid geldt alleen onder de omstandigheden die

de AVG noemt.

Naast bovenstaande rechten heb je het recht om een [klacht](#) omtrent de verwerking van jouw persoonsgegevens in te dienen bij de Autoriteit Persoonsgegevens.

Indien de verwerking van jouw persoonsgegevens is gebaseerd op jouw toestemming, heb je het recht jouw toestemming in te trekken. De intrekking van jouw toestemming doet geen afbreuk aan de rechtmatigheid van de verwerking van jouw persoonsgegevens voorafgaand aan de intrekking van jouw toestemming.

Wil je van (één van) bovenstaande rechten gebruik maken, neem dan contact op met onze functionaris gegevensbescherming.

Pre-DPIA scan

Dit formulier is bedoeld om te bepalen of een DPIA uitgevoerd moet worden t.b.v. een voorgenomen of gewijzigde verwerking van persoonsgegevens. Een DPIA staat voor Data Protection Impact Assessment. Het is een instrument om te beoordelen welke privacyrisico's er voor betrokkenen zijn bij de verwerking van hun persoonsgegevens en hoe deze risico's eventueel beheerst kunnen worden. Een DPIA voer je uit op een categorie van verwerkingen van persoonsgegevens. Vaak komt dit neer op een bepaald werkproces of een nieuw project, waarbij het noodzakelijk is om persoonsgegevens te verwerken. Het is niet altijd nodig om op alle processen of projecten een DPIA uit te voeren.

Wanneer vul je dit formulier in?

Je vult dit formulier in als de volgende criteria van toepassing zijn:

- Als er persoonsgegevens betrokken zijn bij de verwerking;
- Er sprake is van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens of het gaat om persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om in een bestand te worden opgenomen;
- Er een beeld is gevormd van de beoogde (of gewijzigde) verwerking;

Indien je vragen hebt over het onderstaande en behoefte hebt aan toelichting over bepaalde begrippen, kun je contact opnemen met de FG.

Algemene gegevens

1	Algemene gegevens	Beantwoording
1.1	Naam verwerking + toelichting bij verwerking Geef de verwerking een naam die past bij het doel en het proces, zodat meteen duidelijk is waar het over gaat. Liever niet de naam van de applicatie. Bijvoorbeeld: salarisadministratie of afhandelen telefonische klantvraag.	
1.2	Eerder uitgevoerde DPIA? Is er eerder een DPIA uitgevoerd voor deze verwerking? Zo ja, geef aan waarom er mogelijk een nieuwe DPIA moet worden uitgevoerd.	
1.3	Beschrijving verwerking / werkproces Leg uit om welk werkproces het gaat. Bijvoorbeeld: producten ontwikkelen of beantwoorden klachten, onderzoek etc. Indien van toepassing, benoem ook de versie en/of status (concept, in bewerking, voorstel of definitief).	
1.4	Proceseigenaar Geef aan wie de proceseigenaar is.	
1.5	Andere organisaties betrokken? Geef ook aan of er andere organisaties betrokken zijn en wat de rollen per organisatie zijn.	
1.6	Bestaande verwerking? Geef aan of dit een bestaande verwerking is of gaat om een geheel nieuwe verwerking binnen de No.	

Criteria EDPB

De European Data Protection Board (EDPB) heeft een lijst van criteria opgesteld die leiden tot risico verhogende factoren.

2	Is sprake van een van onderstaande factoren?	Ja/Nee	Toelichting
2.1	Evaluatie of scoretoekenning? Het beoordelen van mensen of bedrijven op bepaalde (persoons)kenmerken? Zoals het doen van voorspellingen, profielbepaling van bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene.		
2.2	Geautomatiseerde besluitvorming? Het nemen van <u>geautomatiseerde</u> beslissingen waaraan voor betrokkenen rechtsgevolgen zijn verbonden of vergelijkbare gevolgen hebben. Dit kan leiden tot discriminatie of uitsluiting		
2.3	Stelselmatige monitoring? Verwerking die wordt gebruikt voor het observeren, monitoren of controleren van betrokkenen, incl. via netwerken verzamelde gegevens of stelselmatige monitoring van openbare ruimten. Gaat het om <u>veel</u> gegevens van <u>heel veel</u> mensen en worden de gegevens langdurig of kort gebruikt?		
2.4	Gevoelige gegevens? Dit omvat speciale categorieën van persoonsgegevens zoals gegevens over ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, gezondheid, financiële gegevens, BSN, lidmaatschap van een vakbond of strafrechtelijke veroordelingen of strafbare feiten.		
2.5	Koppeling van datasets? Worden verschillende databronnen/systemen gekoppeld of gecombineerd waardoor data verrijkt wordt?		
2.6	Gegevens van kwetsbare personen? Bijvoorbeeld kinderen, werknemers of kwetsbaardere doelgroepen zoals geesteszieken, asielzoekers, bejaarden, patiënten etc. en in elk geval waarin een onevenwichtigheid in de relatie tussen de positie van de betrokkene en de verwerkingsverantwoordelijke kan worden vastgesteld.		
2.7	Innovatief gebruik/ innovatieve toepassingen? Het gaat hierbij om gebruik van nieuwe, innovatieve technologieën of oplossingen waarbij de consequenties nog niet volledig duidelijk zijn.		
2.8	Blokkering van een recht, dienst of contract? Het gaat hierbij om verwerking van gegevens die tot gevolg kunnen hebben dat iemand geen gebruik kan maken van een dienst, of dat iemand geen contract kan aangaan, wijzigen of weigeren.		
2.9	Doorgifte van persoonsgegevens buiten de EU? Binnen de EU is het niveau van gegevensbescherming gelijk. Buiten de EU gelden andere regels en afspraken.		
Hoe vaak is er met “Ja” geantwoord?			

Criteria Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens heeft een lijst van verwerkingen met hoog risico opgesteld waarvoor een DPIA verplicht moet worden uitgevoerd.

3	Gaat het om een van onderstaande verwerkingen?	Ja/Nee	Toelichting
3.1	Heimelijk onderzoek Grootschalige en/of stelselmatige monitoring van persoonsgegevens waarbij informatie wordt verzameld door middel van onderzoek zonder dat de betrokkene daarvan vooraf op de hoogte te stellen.		
3.2	Zwarte lijsten Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden.		
3.3	Fraudebestrijding/fraudesignalen Grootschalige en/of stelselmatige monitoring van (bijzondere) persoonsgegevens in het kader van fraudebestrijding. Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.		
3.4	Kredietcores Grootschalige en/of stelselmatige monitoring van persoonsgegevens die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen.		
3.5	Financiële situatie Grootschalige en/of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden. Bijvoorbeeld overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen.		
3.6	Gezondheidsgegevens Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid.		
3.7	Samenwerkingsverbanden Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of privacy partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk) met elkaar uitwisselen.		
3.8	Controle werknemers Grootschalige en/of stelselmatige monitoring van persoonsgegevens om activiteiten van werknemers te monitoren. Bijvoorbeeld controle van e-mail en internetgebruik, tijds klokken, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht ten behoeve van diefstal- en fraudebestrijding.		
3.9	Genetische persoonsgegevens Grootschalige en/of stelselmatige monitoring van genetische persoonsgegevens. Bijvoorbeeld DNA-		

	analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken, bio-databanken.		
3.10	Cameratoezicht Grootschalige en/of stelselmatige monitoring met behulp van camera's, webcams of drones.		
3.11	Flexibel cameratoezicht Grootschalig en/of stelselmatig gebruik van flexibel cameratoezicht. Bijvoorbeeld camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten.		
3.12	Locatiegegevens Grootschalige en/of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen. Bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer.		
3.13	Communicatiegegevens Grootschalige en/of stelselmatige monitoring van communicatiegegevens inclusief metadata (de data die niet iets over de inhoud van het bericht zegt, maar over bv het tijdstip) herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker.		
3.14	Internet of things Grootschalige en/of stelselmatige monitoring door verantwoordelijken van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen. Bijvoorbeeld 'internet of things'- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, etc.		
3.15	Profilering Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering). Bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.		
3.16	Observatie en beïnvloeding van gedrag Grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd, verzameld, vastgelegd of beïnvloed wordt, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.		
3.17	Biometrische gegevens Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren.		
	Hoe vaak is er met "Ja" geantwoord?		

Contactgegevens

Contactgegevens	
Naam contactpersoon	
Afdeling contactpersoon	
Datum	

Evt. opmerkingen	
------------------	--

Dank voor het invullen! Stuur dit formulier naar de FG ter controle.



Procedure Rechten van Betrokkenen

Operationele uitwerking

Nationale Ombudsman

Document classificatie

Bedrijfsvertrouwelijk

Versiebeheer

Naam document	Procedure rechten van betrokkenen
Verantwoordelijke	
Auteur	Nationale Ombudsman
Review	Ilionx
Versienummer	0.9 (concept)
Datum eerste versie	
Laatst bijgewerkt	16 november 2020

Wijzigingen			
Datum	Versie	Door	Wijzigingen

Inhoudsopgave

Opbouw document.....	4
1. Rollen en verantwoordelijkheden	5
1.1 Uitgangspunten.....	5
2. Reactietermijnen	5
3 Binnengekomen verzoeken afhandelen.....	6
3.1 Fase 1: Ontvangst van het verzoek	6
3.2 Fase 2: Beoordelen en verwerken van het verzoek.....	8
3.3 Fase 3: Afhandelen verzoek.....	13
4 Encryptie en steekproeven	14
4.1 Hoe pas ik encryptie toe?.....	14
4.2 Hoe hoe voer ik een steekproef uit?	15
5 Bijlagen	16
Bijlage 1 Ontvangstbevestiging	16
Bijlage 2a Herinnering identificatie	16
Bijlage 2b Identiteit niet te verifiëren	16
Bijlage 3 Geen persoonsgegevens aanwezig	17
Bijlage 4: Afwijzen reactie op verzoek van betrokkene	18
Bijlage 5 Positieve reactie: inzage verwerking persoonsgegevens	19
Bijlage bij bijlage 5	20
Bijlage 6: Positieve reactie verzoek rectificatie	23
Bijlage 7: Positieve reactie beperking van de verwerking.....	23

Opbouw document

De Algemene verordening gegevensbescherming (AVG) kent aan betrokkenen een aantal rechten toe, op grond waarvan zij een verzoek kunnen indienen dat betrekking heeft op hun persoonsgegevens. Om (correct en tijdig) gehoor te kunnen geven aan dergelijke verzoeken is een rechten van betrokkenen procedure opgesteld. Deze procedure is in dit document beschreven dat houvast biedt voor een correcte afhandeling.

De procedure voor de behandeling van verzoeken van betrokkenen is opgedeeld in drie fasen, namelijk:

- **Fase 1: Ontvangst van het verzoek (hoofdstuk 3)**
Beschrijving van de stappen die genomen dienen te worden wanneer de Nationale ombudsman een verzoek ontvangt.
- **Fase 2: Beoordelen en verwerken van het verzoek (hoofdstuk 4)**
Beschrijving van de stappen die genomen dienen te worden om het verzoek te beoordelen en vervolgens te verwerken.
- **Fase 3: Afhandeling van het verzoek (hoofdstuk 5)**
Beschrijving van de stappen die genomen dienen te worden om het verzoek administratief af te handelen en de verzoeker de juiste informatie te verschaffen.

1. Rollen en verantwoordelijkheden

Hieronder is uiteengezet wie er zoal betrokken zijn bij een AVG-verzoek binnen de Nationale ombudsman, waarna wordt ingegaan op de belangrijkste uitgangspunten die in acht moeten worden genomen bij de behandeling en beoordeling van dergelijke verzoeken.

I. Verzoeker	II. FG	III. Medewerker	IV. AVG Vertegenwoordiger
I. De natuurlijk persoon die het verzoek indient;			
II. De functionaris gegevensbescherming die als er vragen zijn om hulp gevraagd kan worden;			
III. Degene die indirect bij het verzoek/dossier betrokken is. Stuurt bij ontvangst van het verzoek deze door naar de AVG-vertegenwoordiger en kan om aanvullende informatie vragen;			
IV. Is verantwoordelijk voor het beoordelen en afhandelen van verzoeken.			

1.1 Uitgangspunten

- I. Alle binnengekomen rechten van betrokkene verzoeken worden naar een AVG-vertegenwoordiger verzonden, die deze verder afhandelt.
- II. Voordat het verzoek wordt afgehandeld moet de verzoeker worden geïdentificeerd, bij twijfel kan de FG ingeschakeld worden. [Voordat het verzoek wordt afgehandeld, dient ook de rechtmatigheid van het verzoek te worden vastgesteld.](#)
- III. Alles dat met het verzoek te maken heeft moet als nieuw dossier in het zaakstelsel worden geregistreerd, alle bestaande correspondentie die met het verzoek te maken hebben moeten aan het nieuwe dossier gekoppeld worden.
- IV. De betrokkene moet binnen 5 uiterlijkdagen na ontvangst van het verzoek worden geïnformeerd dat het verzoek in goede orde door Nationale Ombudsman is ontvangen. Zie hier de [standaard reactie](#).
- V. Verzoeken worden in beginsel binnen een maand na ontvangst behandeld. Indien het gaat om veel verzoeken of complexe verzoeken, kan deze termijn met twee maanden verlengd worden. Indien daarvan gebruik wordt gemaakt moet de betrokkene hierover binnen een maand na ontvangst van het verzoek worden geïnformeerd. Ook indien geen gevolg aan het verzoek wordt gegeven dient dat uiterlijk binnen een maand na ontvangst van het verzoek te worden medegedeeld aan de betrokkene.
- VI. De behandeling van een verzoek is kosteloos, tenzij een verzoek kennelijk ongegrond of buitensporig is (met name vanwege het repetitieve karakter ervan). Zie verder artikel 12, lid 5, AVG.

2. Reactietermijnen

Bij het afhandelen van verzoeken is het van belang om onderstaande reactietermijnen in acht te nemen.

Uiterlijk binnen 5 dagen na ontvangst van het verzoek

Dit is de uiterlijke termijn waarbinnen de verzoeker de brief ontvangt waarin staat dat het verzoek door de Nationale ombudsman is ontvangen.

Uiterlijk binnen 2 weken na ontvangst van het verzoek

[Indien de verzoeker niet geïdentificeerd kan worden en ondanks ons verzoek daartoe identificatie uitblijft, dient binnen twee weken na de ontvangstbevestiging een brief gestuurd te worden aan de verzoeker waarin een termijn van vijf dagen wordt gegeven zodat hij/zij alsnog kan identificeren.](#)

Uiterlijk binnen 1 maand na ontvangst van het verzoek

Dit is de reactietermijn waarbinnen gereageerd moet worden bij ontvangst van een verzoek. Deze termijn vangt aan vanaf de dag van binnenkomst.

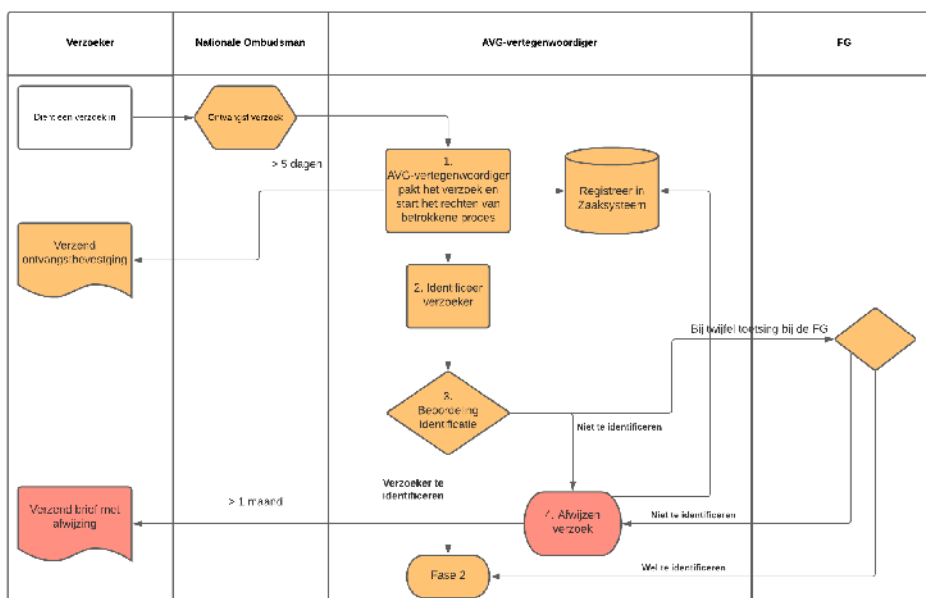
Uiterlijk binnen 2 maanden na ontvangst van het verzoek

De maximale termijn waarmee het afhandelen van een verzoek kan worden verlengd.

3 Binnengekomen verzoeken afhandelen

3.1 Fase 1: Ontvangst van het verzoek

Met opmerkingen [YS1]: Versieon aangepast in zaaksysteem in alle schema's. Onder stap 2 tekst toegevoegd over het uitblijven van identificatie en minderjarigen.



[Fase 1]

Stap 1: AVG-vertegenwoordiger pakt het verzoek op

De behandelend AVG-vertegenwoordiger bevestigt de ontvangst van het verzoek (schriftelijk of digitaal) aan de betrokkene. In de ontvangstbevestiging wordt ook vermeld binnen welke termijn het verzoek wordt afgehandeld (uiterste antwoorddatum).

Verzoeken kunnen op verschillende manieren worden afgehandeld, dit kan zowel schriftelijk, digitaal of mondeling:

1. Een verzoek wordt schriftelijk behandeld. Daarbij geldt als uitgangspunt dat bij digitaal ingediende verzoeken de informatie – voor zover mogelijk – ook digitaal wordt verstrekt, tenzij de betrokkene anderszins verzoekt.
2. Op verzoek van een betrokkene kan de verzochte informatie ook mondeling worden gegeven, op voorwaarde dat de behandelend AVG-vertegenwoordiger zeker weet dat het om betrokkene gaat (zie 2.2 t/m 2.5). In het dossier dient vastgelegd te worden welke informatie is verstrekt aan betrokkene.

- a. De verzoeker wordt geïnformeerd dat het verzoek door de Nationale Ombudsman is ontvangen. Zie in Bijlage 1 de standaard tekst voor de ontvangstbevestiging.
- b. De afhandeling van het verzoek en de informatie die is verstrekt aan de betrokkene dient niet in een bestaand klachtdossier vastgelegd te worden, hiervoor moet altijd een nieuw dossier in het zaaksysteem worden aangemaakt.

Stap 2: Identificeer verzoeker

Wij vragen niet standaard aan iemand om zich te legitimeren door overlegging van zijn/haar legitimatiebewijs. Als de verzoeker aan onderstaande criteria voldoet dan hoeft niet om aanvullende legitimering gevraagd te worden:

- i. De verzoeker en/of intermediair is al bij ons bekend en/of de behandelaar ervan kan verifiëren dat de AVG-vertegenwoordiger met de bij hun bekende verzoeker/intermediair in persoon te maken heeft.
- ii. Eén of meer controlerende vragen te stellen en bijvoorbeeld te informeren naar het dossiernummer.

Mochten er twijfels zijn dan moet de verzoeker gevraagd worden om zich te legitimeren. Hiervoor moet de verzoeker op kantoor langskomen om zijn of haar legitimatiebewijs te laten zien. Als dat bezwaarlijk is, bijvoorbeeld omdat betrokkene ver weg woont, dient gecheckt te worden of de contactpersoon van de betrokken of naburige gemeente bereid is de identificatie voor ons te doen.

Blijft identificatie uit? Verstuur in dat geval een laatste herinnering met de termijn waarbinnen de verzoeker zich alsnog dient te identificeren. Bijlage 2a bevat hiervoor een standaard tekst.

Minderjarigen? Als eraan wordt getwijfeld of de ouder het gezag heeft, kan de ouder gevraagd worden om een recent afschrift van de geboorteakte en een recent uittreksel uit het gezagsregister te overleggen.

Documenten waarmee een verzoeker zich mag identificeren:

- i. Paspoort;
- ii. Nederlandse identiteitskaart;
- iii. ID-kaart of paspoort uit een EER-land;

Stap 2a: Toetsing van ID-bewijzen

Het identificerende document wordt getoetst op vier vragen ("EEGG");

1. is het echt;
2. is het eigen;
3. is het geldig;
4. is het gekwalificeerd.

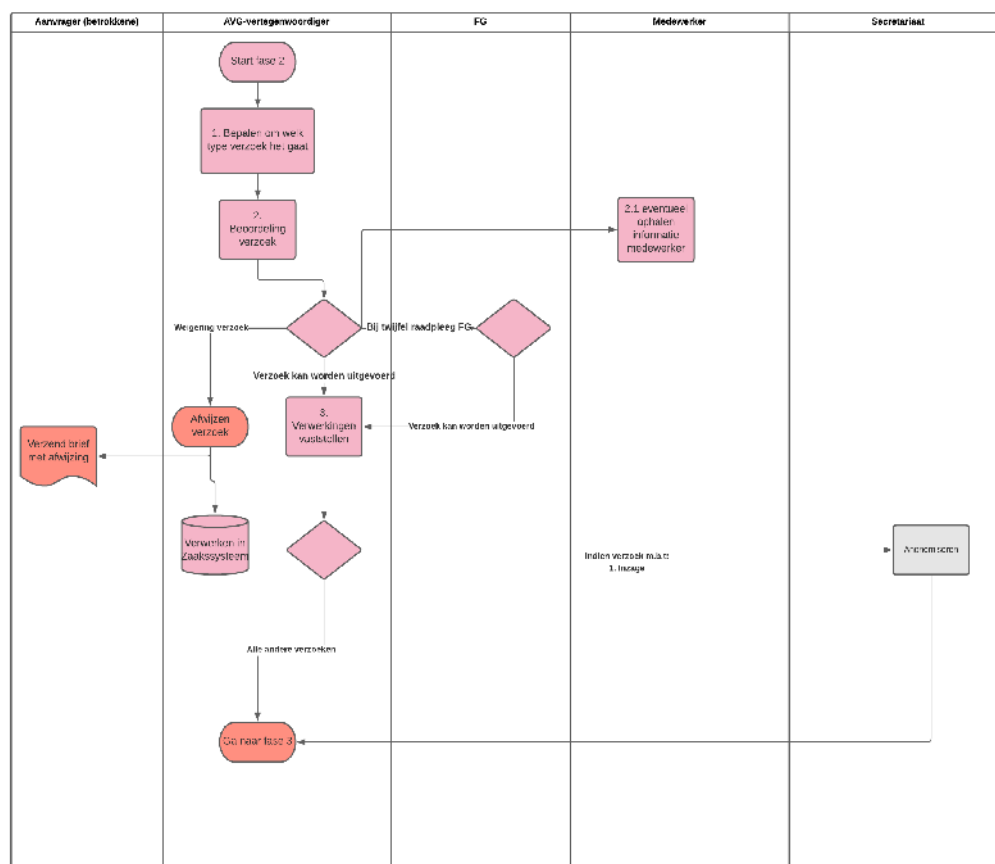
De controle op echtheid behelst een onderzoek naar misbruik, namaak of vervalsing van het ID-bewijs. "Eigen" ziet op de vraag of het ID-bewijs inderdaad betrekking heeft op degene die er gebruik van maakt om zich te identificeren, dan wel is afgegeven aan een andere persoon dan degene die er gebruik van maakt. "Geldig" ziet op de termijn waarvoor het ID-bewijs geldig is. "Gekwalificeerd" wil zeggen het is van de onder stap 2 genoemde documenten is.

Stap 3: Identiteit kan worden vastgesteld

Indien de identiteit van de verzoeker kan worden vastgesteld, dan kan de AVG-Vertegenwoordiger verder naar fase 2 (zie Hoofdstuk 3.2).

3.2 Fase 2: Beoordelen en verwerken van het verzoek

Met opmerkingen [YS2]: Proces van data verzamelen toegevoegd onder 2.1.



Stap 4: Afwijzen verzoek

Als de identiteit van de verzoeker niet kan worden vastgesteld, dan moet de verzoeker binnen 1 maand hierover geïnformeerd worden met de in Bijlage 2 opgenomen beschrijving.

[Fase 2]

Stap 1: Bepalen om welk type verzoek het gaat

Als een verzoek binnenkomt is het van belang om te beoordelen op welk recht het inzageverzoek betrekking heeft. Onderstaande schema kan uitkomst bieden bij het bepalen om welk verzoek het gaat.



De verzoeker kan een beroep doen op een van onderstaande rechten:

TYPE VERZOEK	ARTIKEL AVG
1. Intrekken toestemming verwerking persoonsgegevens	Art. 7 lid 3 AVG
2. Informatie over verwerking persoonsgegevens	Art. 13 en 14 lid 1 AVG
3. Inzage persoonsgegevens	Art. 15 lid 1 AVG
4. Ontvangen kopie persoonsgegevens	Art. 15 lid 3 AVG
5. Rectificatie: correctie / aanvulling persoonsgegevens	Art. 16 AVG
6. Gegevenswissing: verwijdering van persoonsgegevens	Art. 17 AVG
7. Beperking van verwerking persoonsgegevens	Art. 18 AVG
8. Overdracht persoonsgegevens (dataportabiliteit)	Art. 20 AVG
9. Recht van bezwaar	Art. 21 AVG
10. Geautomatiseerde besluitvorming	Art. 22 AVG

Stap 2: Beoordeling verzoek

Alvorens het verzoek in behandeling wordt genomen, dient onderstaande checklist gevolgd te worden. Heb je meer informatie nodig? Kijk dan onder stap 2a en 2b.

Checklist ter voorbereiding op het afhandelen van het verzoek

	VRAAG	TOELICHTING	AVG
1.	Is recentelijk een (inzage)verzoek gedaan?	<u>Zo ja</u> : een verzoek kan worden geweigerd als het kennelijk ongegrond of buitensporig is (vanwege het repetitieve karakter). In dat geval luidt het antwoord op het verzoek dat er geen gevolg aan wordt gegeven. Dit antwoord dient met redenen omkleed te zijn. <u>Zo nee</u> : ga naar vraag 2.	Art. 12 lid 5 AVG
2.	Is het verzoek gespecificeerd?	<u>Zo ja</u> : ga naar vraag 3. <u>Zo nee</u> : vraag om specificatie, met name wanneer een grote hoeveelheid gegevens wordt verwerkt en het niet duidelijk is waar het verzoek van de betrokkene betrekking op heeft. Indien de betrokkene alle persoonsgegevens wil zien en het gaat om een relatief klein dossier, dan kan specificatie achterwege blijven. In andere gevallen, dient het verzoek geweigerd te worden omdat het kennelijk ongegrond of buitensporig is (vanwege het repetitieve karakter). In dat geval luidt het antwoord op het verzoek dat er geen gevolg aan wordt gegeven. Het antwoord dient met redenen omkleed te zijn.	Art. 63 AVG Art. 12 lid 5 AVG
3.	Is sprake van persoonsgegevens?	<u>Zo ja</u> : ga naar vraag 4. <u>Zo nee</u> : het antwoord luidt dat van de betrokkene geen persoonsgegevens worden verwerkt.	
4.	Is de AVG van toepassing op de persoonsgegevens?	<u>Zo ja</u> : ga naar vraag 5. <u>Zo nee</u> : het antwoord luidt dat geen gevolg wordt gegeven aan het verzoek. Dit antwoord dient met redenen omkleed te zijn. AVG is van toepassing op (gedeeltelijk) geautomatiseerde verwerking en op verwerking die in bestand is opgenomen. Een bestand is elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.	Art. 15 AVG
5.	Is de betrokkene al op de hoogte van de persoonsgegevens?	<u>Zo ja</u> : persoonsgegevens waarover de betrokkene al beschikt en waarvan hij zich al een oordeel heeft kunnen vormen, hoeven niet te worden verstrekt. Denk aan: - stukken van of aan (de gemachtigde van) betrokkene; - persoonsgegevens in concept voor zover gelijk aan de definitieve versie; of - een reactie op een vorig verzoek. Het antwoord luidt dan dat geen gevolg wordt gegeven aan het verzoek. <u>Zo nee</u> : ga naar vraag 6.	

VRAAG	TOELICHTING	AVG
6. Is sprake van een weigeringsgrond?	<u>Zo ja</u>: het antwoord luidt dat geen gevolg wordt gegeven aan het verzoek dan wel – als er op een deel van de persoonsgegevens geen weigeringsgrond van toepassing is – dat het verzoek wordt beperkt. Zie onderdeel 2a voor een nadere toelichting van reden om geen gevolg aan een verzoek te geven. <u>Zo niet</u>: het verzoek wordt ingewilligd. N.B. Onder de rechten en vrijheden van "anderen" (art. 23 sub I AVG) moet ook de Nationale ombudsman worden begrepen. Vertrouwelijkheid van informatie kan ook onder het beschermingsbereik van art. 23 sub I AVG vallen.	Art. 23 AVG

Stap 2a: Redenen om geen gevolg te geven aan een verzoek

1. De AVG is van toepassing omdat:	Art. 2 lid 2 sub d AVG
- de gegevens worden verwerkt met het oog op voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten. - de gegevens worden verwerkt met het oog op de tenuitvoerlegging van strafrechtelijke sancties; - de gegevens worden verwerkt in het kader van de bescherming tegen en voorkoming van gevaren openbare veiligheid/nationale veiligheid. - de rechten en vrijheden van anderen dienen te worden beschermd.	
2. Nadat aanvullende gegevens zijn gevraagd, is identificatie van de betrokkene nog steeds niet mogelijk	Art. 11 lid 2 juncto Art. 12 lid 2 AVG
3. Het verzoek is buitensporig (repetitief)	Art. 12 lid 5 AVG

Stap 2b: Redenen om het verzoek te beperken

Een wettelijke grondslag maakt beperking van het verzoek mogelijk, mits die beperking de grondrechten en fundamentele vrijheden onverlet laat en een noodzakelijke en evenredige maatregel is ter waarborging van: a. De nationale veiligheid; b. Landsverdediging; c. Openbare veiligheid; d. Voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, incl. bescherming en voorkoming van gevaren voor openbare veiligheid; e. Doelstellingen van de EU of van een lidstaat (economisch/financieel, monetair, budgettair, fiscaal, volksgezondheid en sociale zekerheid); f. Bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures; g. De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van beroepscodes voor geregelende beroepen; h. Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van openbaar gezag in de bovengenoemde gevallen (m.u.v. punt f.); i. Bescherming van betrokkene of rechten en vrijheden van anderen:	Art. 23 AVG
---	-------------

Preciseringsverzoek

Als na het in behandeling nemen van het verzoek blijkt dat onvoldoende informatie voorhanden is om adequaat op het verzoek te reageren, kan de behandelend medewerker aanvullende informatie vragen, zoals:

- De duiding van het verzoek
- De hoedanigheid van de betrokkene (advocaat, journalist, leverancier, etc.).
- Indien het verzoek een verzoekdossier betreft: of het gaat om een lopende zaak of een afgedane zaak.
- Indien het verzoek geen verzoekdossier betreft: informatie over aard van de betrokkenheid zoals leveranciers, oud-medewerkers, uitzendkrachten, etc.

Peildatum

Als wordt verzocht om informatie over de verwerking van persoonsgegevens, om inzage in de persoonsgegevens en/of om een kopie van de persoonsgegevens, geldt de datum van ontvangst van het verzoek als peildatum. Dat betekent dat het verzoek betrekking heeft op de persoonsgegevens die de

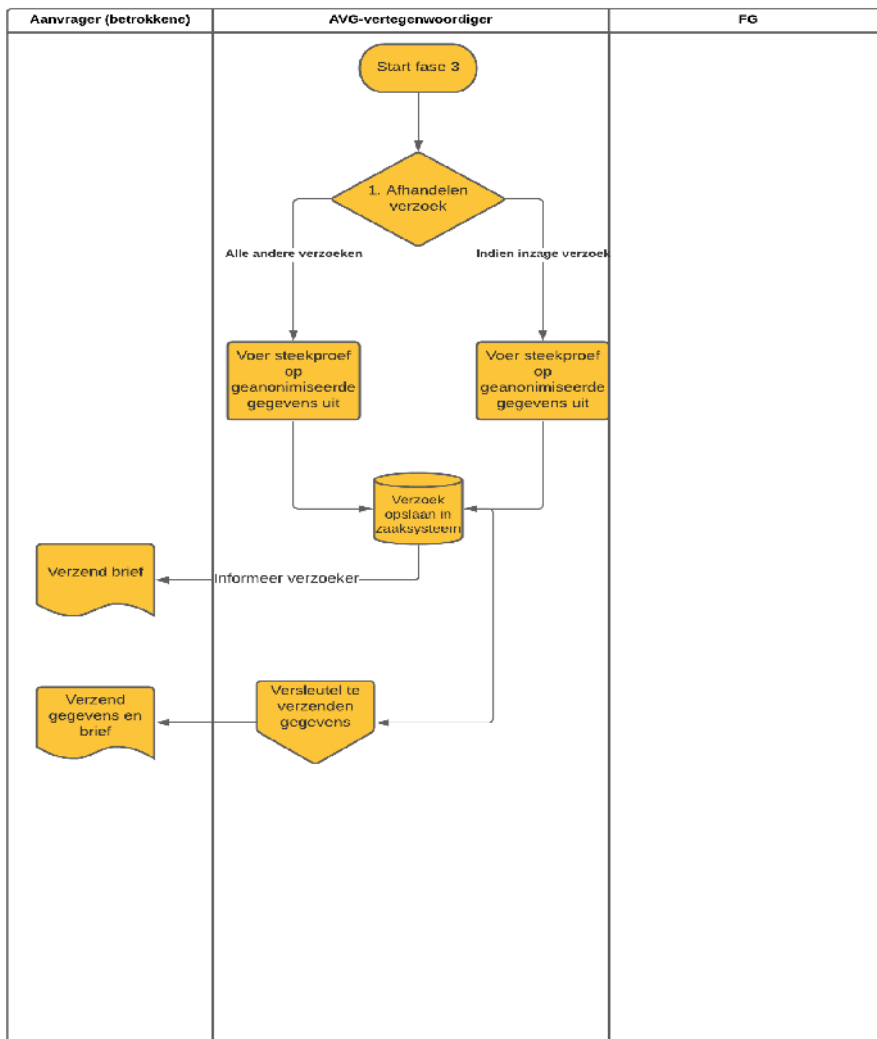
Stap 3: Verwerkingen vaststellen

[interne beschrijving hoe de informatie uit Verseon gehaald dient te worden.]

1. Inzageverzoek
2. Alle andere verzoeken

3.3 Fase 3: Afhandelen verzoek

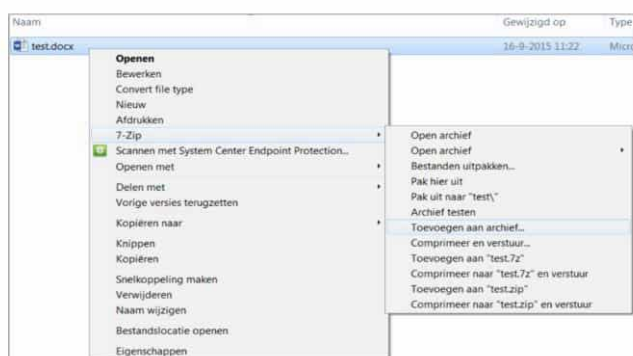
Met opmerkingen [YS3]: Versieon aangepast in zaaksysteem



4 Encryptie en steekproeven

4.1 Hoe pas ik encryptie toe?

1. Start de Windows verkenner en blader naar de map met daarin de te verzenden bestanden (of bestanden plus mappen) die je wilt samenvoegen in een enkel versleuteld en gecomprimeerd bestand. Selecteer dit bestand (of het gewenste setje) en klik er vervolgens met de rechtermuisknop op. Je ziet dan in het contextmenu de optie **7-Zip**, kies hieronder de optie **Toevoegen aan archief**.



2. Controleer volgende instellingen:

- a. Archief formaat: zip.
- b. Codeermethode: AES-256.

3. Open via de browser de website: <https://passwordsgenerator.net/> en selecteer daar als password lengte minimaal 10 karakters.

Password Length:

Include Symbols: ☒ (e.g. @\$%)

Include Numbers: ☒ (e.g. 123456)

Include Lowercase Characters: ☒ (e.g. abcdefgh)

Include Uppercase Characters: ☒ (e.g. ABCDEFGH)

Exclude Similar Characters: ☒ (e.g. l, i, 1, L, o, O)

Exclude Ambiguous Characters: ☐ ({} [] () \ ' " ~ , ; : . < >)

Generate On Your Device: ☒ (do NOT send across the Internet)

Auto-Select: ☐ (select the password automatically)

Save My Preference: ☐ (save all the settings above for later use)

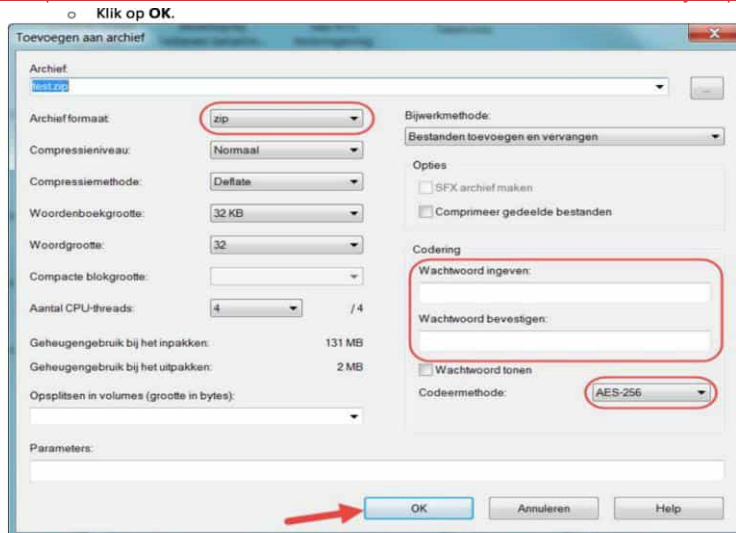
Load My Settings Anywhere: URL to load my settings on other computers quickly

Your New Password:

Remember your password: Remember your password with the first character of each word in this sentence.

4. Zorg dat dezelfde instellingen zijn overgenomen en klik vervolgens op **Generate password**.

5. Kopieer het wachtwoord naar een nieuw Word-document en vul het in bij 7-zip



6. Geef het geselecteerde wachtwoord in en bevestig dit door op OK te drukken.

7. Dit zip-bestand kan je nu beveiligd verzenden als bijlage in een e-mail of delen.

Belangrijk: Voeg de volgende tekst toe aan de te verzenden e-mail:

'De bijlage in deze mail werd beveiligd met een wachtwoord. Om het bestand te kunnen openen, dien je te beschikken over een archiveringstoepassing (7-zip, WinZip, winRAR,...). Indien je hierover niet beschikt kan je de open source 7-zip-software downloaden via <http://www.7-zip.org/download.html>.'

8. Vergeet niet het gebruikte wachtwoord te verzenden aan de geadresseerde, dit kun je door een sms te verzenden naar de verzoeker met daarin het wachtwoord.

9. Verwijder het Word-bestand met daarin het opgeslagen wachtwoord. Het is niet toegestaan om verzonden wachtwoorden op te slaan. Mocht de verzoeker het bericht niet kunnen openen dan kun je hem een nieuw bestand met nieuw wachtwoord toezenden.

4.2 Hoe voer ik een steekproef uit?

Om er zeker van te zijn dan het anonimiseren van de bestanden goed is uitgevoerd is het van belang om een steekproef uit te voeren.

Hoe je dit doet hangt af van het aantal bestanden dat je deelt:

1 - 2 pagina's: controleer 1 pagina

2 - 6 pagina's: controleer 2 niet opeenvolgende pagina's

6+ pagina's: controleer 1/3 van het totaal pagina's, deze mogen niet opeenvolgend zijn.

5 Bijlagen

Bijlage 1 Ontvangstbevestiging

[Niet meezenden: Indien de verzoeker bij zijn aanvraag een legitimatiebewijs heeft meegezonden, vergeet dan niet om te vermelden dat wij het legitimatiebewijs na het vaststellen van zijn identiteit zullen verwijderen.]

De Nationale ombudsman heeft op [datum ontvangst] uw verzoek van [datum verzoek] ontvangen.

Uw verzoek wordt in behandeling genomen en u verneemt zo snel mogelijk, uiterlijk binnen 1 maand, nader bericht.

[Indien de verzoeker niet geïdentificeerd kan worden, kan evt. middels de ontvangstbevestiging gevraagd worden om nadere identificatie].

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Bijlage 2a Herinnering identificatie

De Nationale ombudsman heeft op [datum ontvangstbevestiging] de ontvangst van uw verzoek bevestigd. In deze brief hebben wij tevens aangegeven dat wij uw identiteit niet kunnen verifiëren en hebben wij gevraagd of u zich in persoon wilt laten identificeren op onze locatie met een geldig legitimatiebewijs.

De termijn van een maand waarbinnen de Nationale Ombudsman dient te reageren op uw verzoek op grond van de AVG verloopt op [noem termijn]. Graag willen we u daarom vragen om uiterlijk binnen vijf dagen na ontvangst deze brief deze identificatie alsnog mogelijk te maken zodat we uw verzoek in behandeling kunnen nemen.

Indien u niet in staat bent om langs te komen op locatie, verzoeken wij u vriendelijk om contact met ons op te nemen. U kunt mij bereiken via e-mail: <emailadres> en u kunt mij op<beschikbaarheid in de week> bellen op telefoonnummer (070) <nummer>.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze

Bijlage 2b Identiteit niet te verifiëren

Naar aanleiding van uw verzoek van [datum verzoek] bericht ik u als volgt.

Op basis van artikel 12 AVG zijn wij verplicht om de identiteit te verifiëren op het moment dat er bij ons een verzoek wordt gedaan. Als dit voor ons niet mogelijk is kunnen wij het verzoek helaas niet in behandeling nemen.

Wij kunnen op basis hiervan het door u gedane verzoek helaas niet in behandeling nemen omdat wij uw identiteit niet kunnen verifiëren.

Wij hebben uw verzoek daarom gesloten en zullen deze niet verder oppakken. Als u vragen hebt over dit bericht, dan kunt u mijn bereiken via e-mail: <emailadres>. en u kunt mij op<beschikbaarheid in de week> bellen op telefoonnummer (070) <nummer>.

U kunt ook contact opnemen met de Functionaris gegevensbescherming via avg@nationaleombudsman.nl. Denk er dan aan om uw dossiernummer te vermelden. Uw dossiernummer is <bureaudok nummer>.

Vragen over de afhandeling

Als u niet tevreden bent met de afhandeling van uw verzoek of u een klacht heeft over het gebruik van uw persoonsgegevens door de Nationale ombudsman, dan kunt u daarover contact met ons opnemen of een klacht bij ons indienen. Meer informatie vindt u op de website van de Nationale ombudsman: (www.nationaleombudsman.nl/waarmee-kunnen-wij-u-helpen/uw-privacy).

U kunt ook een klacht indienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Bijlage 3 Geen persoonsgegevens aanwezig

Naar aanleiding van uw verzoek van [datum verzoek] bericht ik u als volgt.

U bent bij de Nationale ombudsman niet bekend. Er worden geen persoonsgegevens van u door de Nationale ombudsman verwerkt.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Bijlage 4: Afwijzen reactie op verzoek van betrokkene

Naar aanleiding van uw verzoek van [datum verzoek] bericht ik u als volgt.

Wij kunnen het door u gedane verzoek niet in behandeling omdat, omdat [kies een van onderstaande redenen van afwijzing].

1. Uw aanvraag is niet ondertekend.
2. Uw verzoek was niet gedateerd.
3. Uw verzoek is [kennelijk] ongegrond op grond van het feit dat [reden]

Bij uitoefening van het recht op inzage

1. De Nationale ombudsman verwerkt uw persoonlijke gegevens niet/heeft geen persoonlijke gegevens die herleidbaar zijn naar u.
2. Toegang tot uw persoonlijke gegevens wordt voorzien door een wettelijke verplichting [specificeer de wet] waarvoor de Nationale ombudsman de verwerking van persoonsgegevens moet uitvoeren.

Bij uitoefening van het recht op rectificatie

1. Uw gegevens die door de Nationale ombudsman worden verwerkt zijn niet inaccuraat.
2. Uw gegevens die door de Nationale ombudsman worden verwerkt zijn niet incompleet

Bij uitoefening van het recht op vergetelheid (het recht om te verwijderen)

1. Uw verzoek is niet gebaseerd op een van de legitieme gronden die zijn uiteengezet in artikel 17 lid 1 van de Algemene Verordening Gegevensbescherming.
2. Uw persoonsgegevens zijn nog steeds nodig voor de doeleinden waarvoor ze oorspronkelijk zijn verzameld of anderszins zijn verwerkt door de Nationale ombudsman, dat wil zeggen voor de volgende doeleinden: [beschrijf gebruik].
3. Uw persoonsgegevens worden niet onrechtmatig verwerkt.
4. De Nationale ombudsman is niet onderworpen aan de wettelijke verplichting om uw persoonsgegevens te verwijderen die in uw verzoek worden vermeld.
5. Uw persoonsgegevens worden niet verzameld met betrekking tot het aanbieden van diensten van de informatiemaatschappij.
6. De verwerking van uw persoonsgegevens is noodzakelijk om te voldoen aan de wettelijke verplichting die voortvloeit uit [vermeld specifieke wet en artikel].
7. De verwerking van uw persoonsgegevens is noodzakelijk teneinde een taak die in het algemeen belang van de Nationale ombudsman wordt uitgevoerd. [beschrijf]
8. De verwerking van uw persoonsgegevens is noodzakelijk met het oog op archiveringsdoeleinden in het algemeen belang, voor wetenschappelijke, historische of statistische doeleinden. De verwijdering van uw persoonsgegevens zal de verwezenlijking van de doeleinden van de verwerking waarschijnlijk ernstig schaden. [te gebruiken in zeer zeldzame gevallen en alleen met toestemming van de FG].
9. De verwerking van uw persoonsgegevens is noodzakelijk voor het instellen, uitoefenen of verdedigen van rechtsvorderingen.

Bij uitoefening van het recht op beperking van de verwerking van persoonsgegevens

1. Uw verzoek is niet gebaseerd op een van de legitieme redenen die zijn uiteengezet in artikel 18 lid 1 van de Algemene Verordening Gegevensbescherming.

2. Uw gegevens zijn niet onrechtmatig verwerkt.
3. De verwerking van uw persoonsgegevens door de Nationale ombudsman is nog steeds noodzakelijk voor de volgende doeleinden [beschrijf gebruik].
4. De Nationale ombudsman streeft naar rechtmatige gronden bij het verwerken van uw persoonsgegevens. Dit wil zeggen [beschrijf].

Bij uitoefening van het recht op het overdragen van persoonsgegevens (data portabiliteit)

- U valt niet onder de voorwaarden van artikel 20 lid 1 van de Algemene Verordening Gegevensbescherming, aangezien:
 - De verwerking van uw persoonsgegevens is niet gebaseerd op uw toestemming.
 - De verwerking van uw persoonsgegevens is niet gebaseerd op een contract
 - De verwerking van uw persoonsgegevens gebeurt niet op een geautomatiseerde wijze.
- Handelen op uw verzoek zou resulteren in een inbreuk op de rechten en vrijheden van derden, namelijk [beschrijf welke derden en de inbreuk].

Indien intrekking van toestemming

1. De verwerking van uw persoonsgegevens door de Nationale ombudsman is niet gebaseerd op uw toestemming.
2. Hoewel de verwerking van uw persoonlijke gegevens door de Nationale ombudsman is gebaseerd op uw toestemming, verwerkt de Nationale ombudsman uw gegevens ook op basis van een andere rechtsgrond, namelijk [beschrijf andere juridische grondslag].

Als u niet tevreden bent met de wijze waarop uw verzoek is afgehandeld, dan heeft u het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens. Meer informatie hierover kunt u vinden op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Bijlage 5 Positieve reactie: inzage verwerking persoonsgegevens

U hebt een verzoek op grond van de Algemene Verordening Gegevensbescherming ingediend. In uw verzoek vraagt u om een kopie van uw persoonsgegevens verwerkt door de Nationale ombudsman.

Reactie op uw verzoek

Uw persoonsgegevens komen voor in de volgende typen verwerkingen:

- <verwerking>
- <verwerking>

In de meegezonden bijlage wordt toegelicht hoe de Nationale ombudsman omgaat met uw persoonsgegevens. De bijlage bevat daarnaast een overzicht van uw persoonsgegevens zoals die door de Nationale ombudsman zijn geregistreerd en een opsomming van uw dossiers. Tot slot zijn afschriften van documenten die uw persoonsgegevens bevatten apart bijgevoegd. Wij hebben om de veiligheid van uw

gegevens te waarborgen deze in een zogenaamd zip-bestand met wachtwoord beveiligd. Het wachtwoord ontvangt in een sms van ons.

Lukt het nu niet om het bestand te openen, dan kunt u op onze website instructies vinden over hoe u het zipbestand kunt openen.

Een klacht indienen

Als u niet tevreden bent met de afhandeling van uw verzoek of u een klacht heeft over het gebruik van uw persoonsgegevens door de Nationale ombudsman, dan kunt u daarover contact met ons opnemen of een klacht bij ons indienen. Meer informatie vindt u op de website van de Nationale ombudsman:

(www.nationaleombudsman.nl/waarmee-kunnen-wij-u-helpen/uw-privacy).

U kunt ook een klacht indienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens

(www.autoriteitpersoonsgegevens.nl).

Hebt u nog vragen?

Als u vragen hebt over dit bericht, dan kunt u mij bereiken via e-mail: <emailadres> en u kunt mij op <beschikbaarheid in de week> bellen op telefoonnummer (070) <nummer>. U kunt ook contact opnemen met de Functionaris gegevensbescherming via avg@nationaleombudsman.nl. Denk er dan aan om uw dossiernummer te vermelden. Uw dossiernummer is <bureaudok nummer>

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Bijlage bij bijlage 5

1. Hoe gaan we om met uw persoonsgegevens?

Gebruik persoonsgegevens

Dient u een klacht bij ons in, dan vragen we u om uw persoonsgegevens. Deze gegevens hebben wij nodig om uw klacht te kunnen behandelen. Verstrekt u de gegevens niet, dan kunnen wij uw klacht niet behandelen.

Verder kunnen uw persoonsgegevens worden gebruikt voor analyse en geanonimiseerde voorbeelden of quotes voor onderzoeken die de ombudsman uit eigen beweging instelt. Het kan ook zijn dat in het kader van een onderzoek uit eigen beweging contact met u wordt opgenomen voor een nadere toelichting of een andere vorm van medewerking.

Daarnaast verwerken wij persoonsgegevens voor dienstverlenende taken, bijvoorbeeld als u een brochure of publicatie van ons wilt ontvangen. Ook verwerken wij uw persoonsgegevens als u bijvoorbeeld solliciteert op een functie bij de Nationale ombudsman. Wij gebruiken uw persoonsgegevens alleen voor het doel waarvoor u ze verstrekt.

Delen van persoonsgegevens

Voor de behandeling van uw klacht kan de Nationale ombudsman gegevens, inclusief persoonsgegevens, delen met de bij uw klacht betrokken (overheids)instanties. Daarom raden wij u aan alleen die informatie op te sturen die wij nodig hebben voor de behandeling van uw klacht.

Voor de dienstverlenende taken wisselen wij geen persoonsgegevens uit met andere instanties. Wij gebruiken uw persoonsgegevens nooit voor commerciële of andere doeleinden dan waarvoor ze zijn verstrekt.

Met organisaties die – in opdracht van de Nationale ombudsman – uw gegevens verwerken, sluiten wij een verwerkersovereenkomst. De Nationale ombudsman blijft verantwoordelijk voor de verwerking van uw gegevens.

Bewaren van persoonsgegevens

De Nationale ombudsman bewaart persoonsgegevens niet langer dan noodzakelijk en wettelijk is toegestaan. De Archiefwet 1995 schrijft de bewaartermijnen voor. In zogenaamde selectielijsten is vastgelegd welke informatie de Nationale ombudsman na verloop van tijd vernietigt of blijvend worden bewaard.

Als er voor specifieke gegevens geen wettelijke bewaartermijn is, bewaren wij de gegevens niet langer dan noodzakelijk is voor de dienstverlening.

2. Overzicht typen verwerkingen

Dit overzicht toont per type verwerking de kenmerken ervan, zoals welke persoonsgegevens worden verwerkt en voor welke doeleinden. Het overzicht is ontleend aan het register van verwerkingen van de Nationale ombudsman, waarin die kenmerken in algemene zin zijn weergegeven. Dat betekent dat in navolgend overzicht mogelijk meer (categorieën van) persoonsgegevens en (categorieën van) ontvangers zijn vermeld dan in uw situatie van toepassing zijn.

Klachtbehandeling <voorbeeld> NB: Deze dient niet meegezonden te worden!

Doel verwerking	Behandeling klachten in de zin van hoofdstuk 9, titel 2 Awb. Het ter behandeling doorzenden van klachten naar het bevoegde bestuursorgaan wanneer nog geen interne klachtbehandeling heeft plaatsgevonden. Het voldoen aan verzoeken om inzage in het dossier door verzoeker (voor zover niet op basis van de AVG).
Rechtsgrondslag	Wettelijke taak
(categorieën) persoonsgegevens	naam, adres, woonplaats, eventuele telefoonnummer en / of e-mailadres. Alle gegevens die een betrokkene relevant acht voor zijn/haar klacht (financieel, relationeel, medisch, strafrechtelijk e.d.)
(categorieën) ontvangers aan wie de gegevens zijn verstrekt	- burgers, - medewerkers van bestuursorgaan betrokken bij klacht, - boa's niet in overheidsdienst, - derden die door één van de partijen bij de klachtbehandeling worden betrokken,

	- verantwoordelijke persoon en/of college bij de desbetreffende bestuursorganen en de door deze gemandateerde medewerkers die bij de klachtbehandeling betrokken zijn, - natuurlijke personen niet zijnde in dienst bij een bestuursorgaan die in opdracht van een bestuursorgaan wettelijke taken uitvoeren of hebben uitgevoerd, - (oud) medewerkers die in dienst zijn bij instanties die wettelijke taken uitvoeren c.q. hebben uitgevoerd voor bestuursorganen.
Bewaartermijn	Volgens de regels van de archiefwet; tussen de 5 jaar en eeuwigdurend (bij overplaatsing naar Nationaal archief). Dossiers die niet worden overgeplaatst naar het Nationaal archief worden na 5 jaar vernietigd.
Verstrekker(s)	Betrokkene, bestuursorganen, officiële en officieuze gemachtigden (zoals familieleden)
Geautomatiseerde besluitvorming?	Nee

3. Overzicht persoonsgegevens

Dit overzicht toont de NAW-gegevens die zijn vastgelegd in het dossier registratie systeem.

Naw nummer	
Naam	
Telefoonnummer	
e-mailadres	
Juridisch Persoon	
Etc...	

4. Overzicht dossiers

Dit overzicht toont de dossiers die in het dossier registratie systeem zijn vastgelegd.

Dossiernummer	type	omschrijving	Vernietigd?

5. Interne notities

Voor zover uw persoonsgegevens voorkomen in interne notities, is kennisgeving ervan niet aan de orde, aangezien die stukken niet vallen onder het toepassingsbereik van het inzagerecht.

Bijlage 6: Positieve reactie verzoek rectificatie

Hartelijk dank voor uw [brief/ e-mail] van [datum].

In overeenstemming met uw verzoek, informeren wij u dat wij de volgende wijzigingen in uw persoonsgegevens hebben aangebracht:

[beschrijf de aangevraagde en geïmplementeerde wijziging]

Deze wijziging gaat van kracht binnen [geschatte tijd]

[Indien van toepassing] Uw verzoek is ook door onze organisatie doorgestuurd naar [elke daadwerkelijke ontvanger van de gegevens vermelden], [tenzij dergelijke communicatie onmogelijk blijkt of onevenredig inspanning vereist].

Hopende u voldoende te hebben geïnformeerd.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,

Bijlage 7: Positieve reactie beperking van de verwerking

Hartelijk dank voor uw [brief/ e-mail] van [datum].

In overeenstemming met uw verzoek, informeren wij u dat wij de volgende wijzigingen in uw persoonsgegevens hebben aangebracht:

[beschrijf de aangevraagde en geïmplementeerde wijziging]

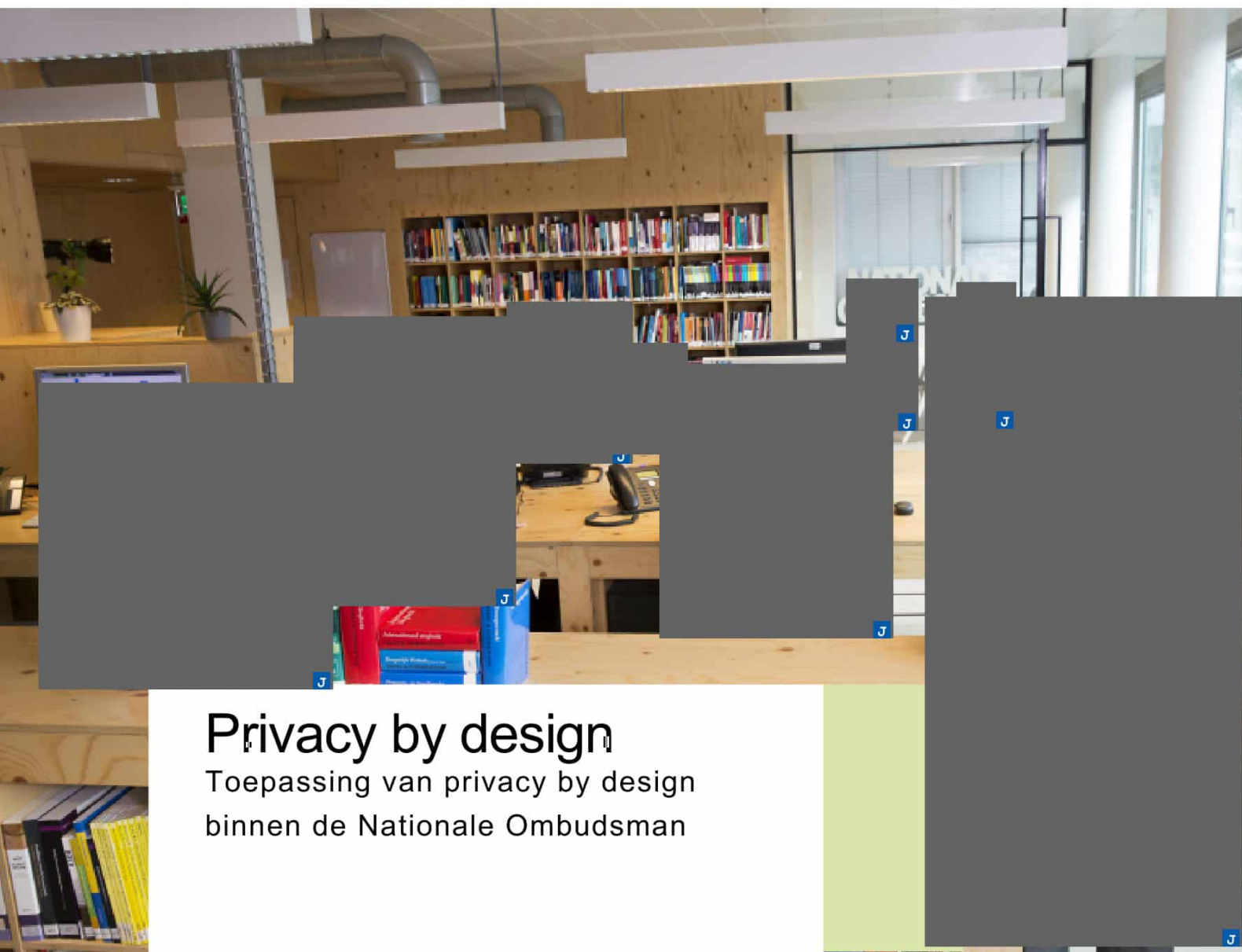
Deze wijziging gaat van kracht binnen [geschatte tijd]

[Indien van toepassing] Uw verzoek is ook door onze organisatie doorgestuurd naar [elke daadwerkelijke ontvanger van de gegevens vermelden], [tenzij dergelijke communicatie onmogelijk blijkt of onevenredig inspanning vereist].

Hopende u voldoende te hebben geïnformeerd.

Met vriendelijke groet,

[naam bevoegd gezag],
namens deze,



Document classificatie

Vertrouwelijk

Versiebeheer

Versienummer	0.4
Gemaakt door	ilionx
Goedgekeurd door	
Datum eerste versie	1-2-2021
Laatst bijgewerkt	23-4-2021

Geschiedenis wijzigingen

Datum	Versie	Aangepast door	Beschrijving van de wijziging
1-2-2021	0.1	ilionx	Eerste opzet
8-2-2021	0.2	ilionx	Review
19-3-2021	0.3		Feedback
23-4-2021	0.4	ilionx	Verwerken feedback

Doel, toepassingsgebied en gebruikers

Dit document is van toepassing op de gehele AVG Governance -scope d.w.z. op alle medewerkers en andere activa die binnen het AVG Governance bereik worden gebruikt, evenals op leveranciers en andere personen buiten de organisatie die in contact komen met systemen en informatie binnen het AVG Governance bereik. Gebruikers van dit document zijn alle medewerkers van de Nationale ombudsman evenals alle bovengenoemde personen.

Referentiedocumenten en/of applicaties

- CIP- Handleiding Privacy by Design
- VNG- Handreiking Privacy by Design

- [REDACTED] - Privacyontwerpstrategieën van (Het blauwe boekje)
- EDPB - Guidelines 4/2019 on Article 25 Data Protection by Design and by Default version 2.0 adopted on 20 october 2020.

Inhoudsopgave

1	Inleiding	5
1.1	Privacy by Design	5
1.1.1	De zeven principes van privacy by design	5
1.2	Juridisch kader	7
1.3	Passende technische en organisatorische maatregelen	9
2	Privacyontwerpstrategieën	11
3	Toepassen PbD.....	16

1 Inleiding

1.1 Privacy by Design

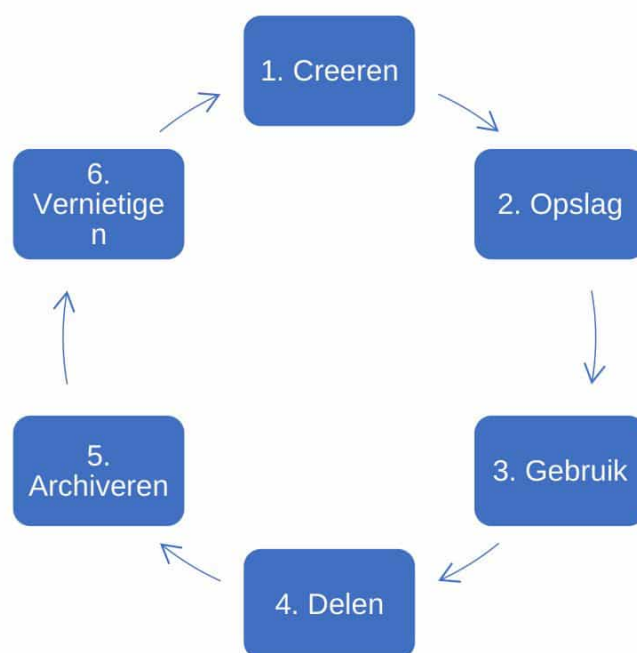
Privacy by design (PbD) is gericht op het proactief meenemen van privacybescherming in de ontwerpfase bij het uitvoeren van projecten. Het toepassen van PbD borgt dat systeemarchitecten, ontwerpers en ontwikkelaars privacy criteria toepassen waarmee de rechten en vrijheden van betrokkenen kunnen worden geborgd.

Het toepassen van PbD levert een organisatie meerdere voordelen op, zo leidt het toepassen bijvoorbeeld tot het gemakkelijker kunnen uitvoeren van een verzoek van een betrokkene om gebruik om te maken van zijn rechten, het kunnen toepassen en handhaven van de dataretentietermijnen en het toepassen van privacy beveiligingsmaatregelen.

Om PbD toe te passen wordt dit gekoppeld aan de zogenaamde Data Levens Cyclus Management (DLM).

DLM en PbD

1. Op welke wijze ontvangen wij de informatie.
2. Waar wordt de informatie opgeslagen?
3. Hoe en wie gaat de informatie gebruiken?
4. Met wie wordt de informatie gedeeld?
5. Dient de informatie gearhiveerd te worden?
6. Hoe gaan we om met de vernietiging van de informatie?



1.1.1 De zeven principes van privacy by design

Privacy by design is gebaseerd op de volgende zeven fundamentele principes:



1. Proactief en preventief; niet reactief en herstellend

PbD kenmerkt zich door het nemen van proactieve maatregelen in plaats van reactieve. Het anticipeert op en voorkomt inbreuken op iemands privacy voordat deze feitelijk plaatsvinden.

2. Privacy criteria gelden per default

PbD streeft naar een maximale privacy door te verzekeren dat persoonsgegevens in een IT-systeem of handelingspraktijk de privacy automatisch afdoende beschermd is. Ook als een betrokkene niets onderneemt zal toch zijn privacy zijn gewaarborgd. Van het individu wordt geen specifieke actie gevraagd om zijn privacy te beschermen; dat is standaard ingebouwd in het systeem.

3. Privacy maatregelen zijn geïntegreerd in het ontwerp

PbD is geïntegreerd in het ontwerp en de architectuur van IT-systemen en handelingspraktijken. Het is er niet als een extraatje of een lastig los onderdeel aan vastgeplakt, bijvoorbeeld nadat er een privacy schending heeft plaatsgevonden of zwakke plekken zijn ontdekt. Als resultaat hiervan is privacy een essentieel onderdeel van de kernfunctionaliteit.

4. Volledige functionaliteit

Een gebruiker moet de volledige functionaliteit van een product of dienst kunnen gebruiken zonder dat hij daarvoor (een deel van) zijn privacy moet inleveren. De zogenoemde cookie-wall is een voorbeeld hoe het niet moet. Hierbij kan de gebruiker de website niet bezoeken als hij geen cookies accepteert.

5. Bescherming tijdens de volledige datalevenscyclus

Privacy van gegevens strekt zich uit over de gehele levenscyclus van de persoonsgegevens van begin tot eind: verzamelen, opslag en de uiteindelijke verwijdering van gegevens. Verwerkingen van persoonsgegevens kunnen in de loop van de tijd wijzigen. Bij het ontwerpen van systemen moet daarom rekening



gehouden worden met veranderende omstandigheden. Hiervoor is het nodig dat de werking van de privacy maatregelen gemonitord kan worden (ten behoeve van zichtbaarheid en transparantie) en dat het ontwerp veranderingen gemakkelijk aan kan. Deze veranderbaarheid start al bij de architectuurkeuzes in het ontwerp en zelfs nog wel eerder: als bewust gekozen vereiste in het beleid.

6. Inzicht en transparantie

Inzicht en transparantie over hoe persoonsgegevens worden verwerkt is binnen de wet- en regelgeving een criterium en moet mogelijk gemaakt worden voor de betrokkene, de eigen organisatie en toezichthouders.

7. Respect voor de privacy van de gebruiker

Privacy by Design heeft zijn doel pas bereikt, wanneer het (binnen de context van de verwerking van persoonsgegevens) daadwerkelijk zorgdraagt voor de bescherming van de persoonlijke levenssfeer. Niet het toepassen of uitvoeren van een maatregel is hierbij leidend, maar het beoogde resultaat voor de betrokkene. Bij iedere maatregel moet daarom verder gekeken worden dan alleen het uitvoeren ervan: er moet vastgesteld worden of het beoogde resultaat voor de betrokkene zich daadwerkelijk voordoet. Het correctierecht, het laten staken van de verwerking van zijn of haar gegevens en het uitwissen van de gevolgen voor de persoonlijke levenssfeer van de betrokkene zijn voorbeelden, waarbij de persoonlijke levenssfeer kan worden beschermd. De uitdaging: balans vinden tussen met zo min mogelijk maatregelen het meeste effect weten te bereiken.

1.2 Juridisch kader

De No is op grond van artikel 25 van de AVG verplicht passende technische en organisatorische maatregelen te treffen die (1) ontworpen zijn om de gegevensbeschermingsbeginselen op een effectieve manier te implementeren (ontwerp/design) en die (2) met behulp van standaardinstellingen de nodige waarborgen bevatten ter naleving van de voorschriften van de AVG en ter bescherming van de rechten van betrokkenen (standaard/default).



Artikel 25 AVG

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Privacy by design

De AVG dwingt in lid 1 van artikel 25 privacy by design af, of te wel: gegevensbescherming door ontwerp. Dit houdt in dat er al bij de start van het ontwerp van een product, dienst, informatiesysteem of proces rekening wordt gehouden met privacy. Dat kan al door na te denken over de noodzakelijkheid van het opslaan van de betreffende persoonsgegevens; welke gegevens zijn echt nodig en welke niet? Daarnaast moet rekening worden gehouden met de hele levenscyclus van de data: opslag, wijziging en verwijdering.

Privacy by default

Naast privacy by design verplicht de AVG in lid 2 van artikel 25 tot privacy by default (standaardinstellingen). Dit ziet bijvoorbeeld toe op de keuzes die worden gemaakt over standaardconfiguraties in bijvoorbeeld softwareapplicaties, computerprogramma's en apparaten. Bij standaardinstellingen kan onder meer worden gedacht aan de mogelijkheid voor betrokkenen om in te grijpen in hun persoonsgegevensverwerking, het automatisch op gezette tijden informatie geven over welke persoonsgegevens zijn opgeslagen, pseudonimisering van persoonsgegevens en systemen voor opsporing van schadelijke software.



1.3 Passende technische en organisatorische maatregelen

De AVG schrijft niet welke maatregelen genomen moeten worden in het kader van privacy by design. Het is aan de verwerkingsverantwoordelijken om aan te tonen dat bij de gegevensverwerking effectieve passende technische en organisatorische maatregelen zijn ingevoerd. Voorbeelden hiervan zijn encryptie, pseudonimisering, anonimisering, privacy by default en beperking van de opslag van gegevens.

De te nemen maatregelen dienen in de eerste plaats te waarborgen dat de beginselen uit artikel 5 van de AVG op een effectieve manier worden geïmplementeerd. Uit lid 1 van artikel 25 AVG volgt dat hierbij rekening dient te worden gehouden met de volgende elementen:

- stand van de techniek: (ISO)-standaarden en certificering kunnen een rol spelen bij de indicatie van de moderne stand van de techniek;
- Implementatiekosten;
- aard, omvang, context en doel: verwerking van bijvoorbeeld bijzondere persoonsgegevens vergt specifieke maatregelen;
- risico's rechten en vrijheden betrokkenen: hoe waarschijnlijk is het risico dat voor een betrokkene optreedt en welke maatregelen kunnen genomen worden om deze risico's te minimaliseren?

In de tweede plaats dienen de maatregelen te waarborgen dat de voorschriften uit de AVG en de rechten van betrokkenen worden beschermd middels standaardinstellingen (privacy by default). Art. 25 lid 2 AVG bevat vier elementen waarmee de verwerkingsverantwoordelijke kan bepalen welke technische en organisatorische maatregelen passend zijn voor privacy by default, namelijk:

- Hoeveelheid: dit element heeft naast een kwantitatief aspect ook een kwalitatief aspect. Dit laatste houdt in dat ook de types, categorieën en gedetailleerdheid van persoonsgegevens in beschouwing moet worden genomen.
- Data minimalistatie waarin persoonsgegevens worden verwerkt: dit element ziet toe op het vereiste dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk voor het doel van de gegevensverwerking.



Daarbij dient rekening te worden gehouden met de redelijke verwachtingen van betrokkenen.

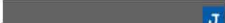
- Opslagtermijn: middels standaardinstellingen dient bewerkstelligd te worden dat persoonsgegevens niet langer bewaard blijven dan noodzakelijk is voor het doel. Denk hierbij aan systematische procedures voor verwijdering dan wel anonimisering van persoonsgegevens.
- Toegankelijkheid: art. 25, lid 2 dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk wordt gemaakt. Ter effectuering moet de verwerkingsverantwoordelijke hiervoor standaardinstellingen inbouwen. Daarnaast moet de verwerkingsverantwoordelijke via standaardinstellingen als autorisatie bewerkstelligen dat persoonsgegevens in een organisatie niet voor iedereen toegankelijk zijn.



2 Privacyontwerpstrategieën

De privacyontwerpstrategieën zijn ontwikkeld met als doel het borgen van privacybescherming in gegevensverwerkingen en hieraan gekoppelde informatiesystemen. Deze strategieën stellen vanuit een technisch en organisatorisch perspectief doelen die - als ze bereikt worden - de privacy van het systeem verbeteren en kunnen worden gezien als vragen die gesteld kunnen worden tijdens het ontwikkelproces. Daarnaast zijn de privacy strategieën niet alleen toepasbaar bij het zelf ontwikkelen van systemen, maar kunnen deze ook dienen als een pakket van eisen voor de aanschaf van systemen.¹ De strategieën zijn onderverdeeld in vier datageoriënteerde strategieën (minimaliseer, scheid, abstraheer en verberg) en vier procesgeoriënteerde strategieën (informeer, geef controle, dwing af en toon aan). Onderzoek voor iedere strategie hoe die van toepassing zou kunnen zijn op de gegevensverwerking.

	Strategie	Criterium	Specificatie
1	Minimaliseren	Selecteer enkel strikt noodzakelijke personen of gegevens. Niet-noodzakelijke personen of gegevens dienen van te voren uitgesloten te worden.	De verzameling van persoonsgegevens dient beperkt te worden tot het minimum dat relevant, evenredig en noodzakelijk is voor de geïdentificeerde doeleinden. Het minimaliseren van persoonsgegevens kan door van minder personen gegevens te verwerken of per persoon minder gegevens te verwerken. - Selecteer alleen relevante personen of gegevens en alleen dat wat strikt noodzakelijk is. Bepaal daarom vooraf welke personen of gegevens strikt noodzakelijk zijn vanuit het doel van de gegevensverwerking, en verzamel enkel die gegevens. Verzamel en bewaar gegevens alleen als ze aan het selectiecriterium voldoen. Voorbeeld: Gebruik een whitelist waarbij je definieert welke gegevens verwerkt mogen worden. Een bepaald gegeven mag alleen

¹ Het blauwe boekje van 



			verwerkt worden als deze op de lijst voorkomt. Voor niet-noodzakelijke personen of gegevens kan een blacklist worden gedefinieerd van gegevens die niet verwerkt mogen worden. - Sluit uit welke personen of gegevens niet relevant/noodzakelijk zijn en verzamel die gegevens niet of verwijder ze direct nadat ze zijn binnengekomen. - Verwijder gegevens die niet langer nodig zijn. Bepaal van te voren hoe lang gegevens nodig zijn en zorg ervoor dat ze automatisch verwijderd kunnen worden. Als het een specifiek veld uit een record betreft dat nog wel bewaard moet worden, zet dat veld dan op een default waarde.
2	Scheiden	Verzamel en leg persoonsgegevens zo veel mogelijk vast in losse verwerkingen en verwerk de persoonsgegevens zoveel mogelijk in verschillende fysieke locaties	Een andere belangrijke strategie is om verschillende persoonsgegevens gescheiden (logisch dan wel fysiek) van elkaar te verwerken. Dit maakt het moeilijker om verschillende gegevens met elkaar te combineren. Door gegevens uit verschillende contexten apart te verwerken, is het risico kleiner dat gegevens uit de ene context in de andere context bekend worden. - Verzamel of verwerk (indien mogelijk) de persoonsgegevens in verschillende logisch gescheiden, databases of systemen. Het gaat hier om het vinden van een balans tussen welke gegevens centraal beschikbaar zijn en welke gegevens op apparaten staan. - Hoe meer gegevens gescheiden van elkaar op apparaten opgeslagen zijn, hoe privacyvriendelijker. Aandachtspunt Grotere scheiding zorgt mogelijk ook voor problemen bij de vindbaarheid van gegevens. Als de gegevens per (sub)verwerking worden opgeslagen en er



			sprake is van veel mogelijke vormen van verwerking, dan kan het lastig zijn om bij een verzoek tot inzage, wissing e.d. de gegevens van alle verwerkingen en applicaties terug te vinden en er zeker van te zijn dat je niets mist. Maak bewust een afweging tussen het scheiden of juist het verbinden van gegevens.
3	Abstraheren	Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt	Dit richt zich op de vraag in welke mate van detail persoonsgegevens verwerkt moeten worden. - Aggregeer informatie over categorieën personen in plaats van per individu (waar mogelijk). Stel bijvoorbeeld een groepsprofiel op met de gemiddelde waarde van de gegevens van alle mensen van een bepaalde leeftijd of een bepaald postcodegebied. - Vat gedetailleerde informatie samen in meer algemene gegevens. Registreer bijvoorbeeld een leeftijdscategorie in plaats van een geboortedatum, of een woonplaats in plaats van het precieze adres. (In veel gevallen bijvoorbeeld om te controleren of iemand meerderjarig is, is enkel de leeftijd en niet de specifieke geboortedatum van belang. In plaats van de geboortedatum te registreren kan je volstaan met de vermelding 'ouder dan 18 jaar' - Ruis toevoegen, verstoren: gebruik niet de precieze waarde van een gegeven. Gebruik een benadering van de waarde of pas de waarde aan met een kleine hoeveelheid ruis.
4	Verbergen	Bescherm persoonsgegevens of maak ze onherleidbaar of beperkt beschikbaar.	Deze belangrijke strategie richt zich op de vertrouwelijkheid, herleidbaarheid en beschikbaarheid van persoonlijke gegevens - Beperk toegang tot persoonsgegevens: voer strikte maatregelen in voor toegangscontrole.



			- Maak data ongrijpbaar voor derden: versleutel data zodat ze onleesbaar worden zonder de sleutel. Bijv. hash persoonsgegevens om er pseudoniemen van te maken. - Verbreek de link en de correlatie tussen gebeurtenissen, personen en gegevens. Verwijder direct identificerende gegevens. - Maak data onherleidbaar: door persoonsgegevens met elkaar te mengen of anonimiseren.
5	Informereren	Informeert gebruikers op tijd en adequaat over de verwerking van hun persoonsgegevens	- Informeert: Bepaal de wettelijke eisen voor wanneer informatie aan de betrokkenen moet worden verstrekt (bijvoorbeeld voorafgaand aan de verwerking, binnen een bepaalde tijd vanaf het moment waarop deze wordt gevraagd, et cetera) en voor het type informatie dat moet worden verstrekt. - Verstrek bijgewerkte informatie als de doeleinden voor de verwerking van persoonsgegevens worden gewijzigd of uitgebreid. - Leg uit: Verstrek de informatie aan betrokkenen in een tijdige, beknopte, volledige, transparante, begrijpelijke en gemakkelijk toegankelijke vorm, afhankelijk van de doelgroep. Pictogrammen en afbeeldingen kunnen de betrokkenen helpen door een visueel overzicht te geven van de beoogde verwerking. - Waarschuw: indien persoonsgegevens met derden gedeeld zullen worden of als ze gelekt zijn.
6	Controle	Geef gebruikers controle over de verwerking van hun persoonsgegevens	- Vraag toestemming wanneer geen beroep gedaan kan worden op de andere grondslagen. - Geef gebruikers de mogelijkheid om persoonsgegevens te corrigeren en te (laten) verwijderen indien deze niet noodzakelijk zijn.
7	Afdwingen	Commiteer je aan een privacy vriendelijke	- Bepaal per verwerking het doel, en de (juridische) grondslag: is er een gerechtvaardigd belang, taak van



		verwerking van persoonsgegevens en dwing deze af	algemeen belang of moet er om toestemming gevraagd worden? - Dwing het beleid af met alle noodzakelijke technische en organisatorische maatregelen. Het gebruik van speciale categorieën persoonsgegevens kan worden onderworpen aan strengere maatregelen. Of het een speciale categorie persoonsgegevens betreft hangt af van kenmerken, bijvoorbeeld door de aard van de persoonsgegevens (bijvoorbeeld medische informatie) of door de betrokkene (bijvoorbeeld persoonsgegevens met betrekking tot kinderen). - Neem passende maatregelen, rekening houdend met de beschikbare technologie, om derden op de hoogte te brengen van elke wijziging of intrekking van toestemming of bezwaren met betrekking tot de gedeelde persoonsgegevens. - Zorg dat derden (de zogenaamde 'verwerkers') aan de door de organisatie gestelde eisen voldoen d.m.v. afspraken in verwerkersovereenkomsten en het naderhand hierop auditen ter controle - Beheer: Controleer het privacybeleid en de implementatie daarvan, regelmatig, en pas waar nodig aan. Stel vooraf eisen op, en toets hier aan.
8	Aantonen	Toon aan dat je op een privacy vriendelijke wijze persoonsgegevens verwerkt	- Documenteer alle (belangrijke) stappen die worden genomen. Leg beslissingen vast, en motiveer deze. Verzamel logs - Audit: audits op logs maar denk ook aan (pre) DPIA's en het uitvoeren van audits bij verwerkers. - Rapporteer de resultaten van de audits / DPIA's aan de FG.



3 Toepassen PbD

Om PbD goed toe te kunnen passen moet dit in elke fase van de levenscyclus van de verwerking worden toegepast. Ieder fase vraagt om aandacht voor privacy. Om dit te kunnen borgen is door de No een dashboard (checklist) ontwikkeld die als leidraad dient bij het toepassen van PbD binnen projecten. Deze checklist dient door de applicatieeigenaar en/of proceseigenaar voor de start van het project te worden ingevuld. De resultaten hiervan dienen enerzijds als leidraad en anderszijds als terugkoppeling naar de FG die indien nodig kan adviseren over mogelijk (nog) te nemen acties.

De uitkomsten van het PbD dashboard worden in GRC geregistreerd.



Procesbeschrijving

AVG-VERZOEKEN

1	INLEIDING	2
2	RECHTEN VAN BETROKKENEN.....	3
3	AANDACHTSPUNTEN	4
4	PROCES IN DETAIL.....	6
4.1	REGISTRATIE VAN AVG-VERZOEK IN DJUMA	8
4.2	UITVOEREN VAN CONTROLES.....	8
4.2.1	<i>Controle identiteit.....</i>	8
4.2.2	<i>Controle veelvragers</i>	9
4.3	VERSTUREN ONTVANGSTBEVESTIGING.....	9
4.4	SPECIFICATIE VERZOEK	9
4.5	GEEN GEVOLG GEVEN AAN HET VERZOEK/HET VERZOEK WORDT BEPERKT	9
4.6	BEHANDELING AVG-VERZOEK.....	11
4.6.1	<i>Inzageverzoeken</i>	11
4.6.1.1	Verzamelen van persoonsgegevens	11
4.6.1.2	Antwoord (inhoudelijk) op het verzoek.....	12
4.6.2	<i>Verwijderverzoek</i>	14
4.6.2.1	Beoordelen verwijderverzoek	14
4.6.2.2	Inwilligen verwijderverzoek.....	15
4.6.2.3	Verzoek beantwoorden	15
4.6.3	<i>Verzoek tot rectificatie.....</i>	15
4.6.3.1	Beoordelen verzoek tot rectificatie	15
4.6.3.2	Inwilligen verzoek tot rectificatie	16
4.6.3.3	Verzoek beantwoorden	16
4.6.4	<i>Verzoek tot bezwaar</i>	16
4.6.4.1	Beoordelen verzoek tot bezwaar	16
4.6.4.2	Inwilligen verzoek tot bezwaar.....	16
4.6.4.3	Verzoek beantwoorden	16
4.6.5	<i>Verzoek tot beperking.....</i>	17
4.6.5.1	Beoordelen verzoek tot beperking	17
4.6.5.2	Inwilligen verzoek tot beperking	17
4.6.5.3	Verzoek beantwoorden	17
4.6.6	<i>Verzoek tot overdraagbaarheid (dataportabiliteit)</i>	17
4.6.6.1	Beoordelen verzoek tot overdraagbaarheid.....	17
4.6.6.2	Inwilligen verzoek tot overdraagbaarheid.....	17
4.6.6.3	Verzoek beantwoorden	17
4.6.7	<i>Recht om niet onderworpen te zijn aan geautomatiseerde besluitvorming.....</i>	18
	BIJLAGE A BEGRIPPENLIJST.....	19
	BIJLAGE B MODELTEKSTEN.....	20
	ONTVANGSTBEVESTIGING.....	20
	BESLUIT GEEN GEVOLG/BEPERKING AVG-VERZOEK.....	21
	ANTWOORDEN OP HET AVG-VERZOEK.....	22

1 Inleiding

De Algemene Verordening Gegevensbescherming (AVG) is een Europese wet die de privacy rechten van individuen regelt en de manier waarop organisaties persoonsgegevens verwerken.

In artikel 13 t/m 22 staan alle rechten van betrokkene. In het kader van de AVG zijn de betrokkenen degenen van wie persoonsgegevens worden verwerkt. Met betrekking tot de verwerking van hun persoonsgegevens hebben de betrokkenen een aantal rechten onder de AVG. Wanneer iemand gebruik maakt van (een) deze rechten dan spreken we van een verzoek van een betrokkene (in dit document wordt hiervoor de term 'AVG-verzoek' gebruikt).

Afhankelijk van de reikwijdte en complexiteit van een verzoek op basis van genoemde artikelen uit de AVG kan afhandeling hiervan een zeer tijdsintensieve onderneming zijn waarbij een aantal stappen doorlopen moet worden.

Om een verzoek van een betrokkene uniform, efficiënt en binnen de wettelijke reactietermijn te kunnen afhandelen is een duidelijke procesbeschrijving nodig.

Het proces met betrekking tot de rechten van de betrokkene is in dit document beschreven.

2 Rechten van betrokkenen

De AVG kent de volgende rechten van betrokkenen:

Recht op informatie (art. 13 en 14 AVG): Organisaties moeten betrokkenen informeren over de verwerking van hun persoonsgegevens. Dit omvat details zoals de doeleinden van de verwerking, de categorieën van persoonsgegevens die worden verwerkt, en de rechten van de betrokkenen.

Recht op inzage (art. 15 AVG): Betrokkenen hebben het recht om te weten of hun persoonsgegevens worden verwerkt, en zo ja, om deze gegevens in te zien.

Recht op rectificatie (art. 16 AVG): Betrokkenen hebben het recht om onjuiste persoonsgegevens te laten corrigeren en onvolledige gegevens aan te vullen.

Recht op gegevenswissing (art. 17 AVG): Betrokkenen hebben in bepaalde gevallen het recht om hun persoonsgegevens te laten wissen.

Recht op beperking van de verwerking (art. 18 AVG): Betrokkenen hebben onder bepaalde omstandigheden het recht om de verwerking van hun persoonsgegevens te beperken.

Recht van overdraagbaarheid (dataportabiliteit) (art. 20 AVG): Betrokkenen hebben het recht om hun persoonsgegevens te ontvangen in een gestructureerd, veelgebruikt en machine leesbaar formaat, en ze hebben het recht om deze gegevens over te dragen aan een andere verwerkingsverantwoordelijke.

Recht van bezwaar (art. 21 AVG): Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens op basis van bepaalde gronden.

Recht om niet onderworpen te zijn aan geautomatiseerde besluitvorming (art. 22 AVG): Betrokkenen hebben het recht om niet onderworpen te worden aan besluiten die uitsluitend gebaseerd zijn op geautomatiseerde verwerking, inclusief profilering, tenzij dit gerechtvaardigd is en bepaalde voorwaarden zijn vervuld.

3 Aandachtspunten

PDCA-cyclus

Deze procesbeschrijving is onderdeel van de AVG-verbetercyclus. Dit betekent dat het proces periodiek wordt getoetst aan de praktijkervaringen, wijzigingen in wet- en regelgeving en de inrichting van de organisatie.

De Privacy officer (PO) behandelt AVG-verzoeken

Om de uniformiteit van het afhandelen van verzoeken te bewaken en vanwege de korte wettelijke behandeltermijn worden de verzoeken door de PO behandeld.

De FG toetst de behandeling van een AVG-verzoek en ondertekent de begeleidende brief bij beantwoording van een AVG-verzoek.

Registratie in Djuma

AVG-verzoeken worden geregistreerd in Djuma op een uniforme wijze. Hierdoor is eenvoudig te rapporteren over AVG-verzoeken. Voor registratie van AVG-verzoeken wordt het zaaktype 'AVG' gebruikt.

Antimisbruikbepaling

De AVG bevat een antimisbruikbepaling. Dit betekent dat een verwerkingsverantwoordelijke mag weigeren gevolg te geven aan een AVG-verzoek als bedoeld in artikelen 13 t/m 22 als het verzoek kennelijk ongegrond of buitensporig is.

Van kennelijk ongegrond is sprake als er duidelijk niet is voldaan aan de randvoorwaarden voor een verzoek.

Een verzoek is buitensporig als het een disproportionele last legt op de verwerkingsverantwoordelijke, bijvoorbeeld wanneer het te vaak wordt ingediend of zeer omvangrijke verzoeken betreft. Let wel, dat een verzoek duur, arbeidsintensief of complex is, zal geen argument zijn om te weigeren. In geval van weigering moet de verwerkingsverantwoordelijke aantonen dat het verzoek buitensporig of kennelijk ongegrond is.

Peildatum

Als wordt verzocht om informatie over de verwerking van persoonsgegevens of om inzage in de persoonsgegevens, geldt de datum van ontvangst van het verzoek als peildatum. Dat betekent dat het verzoek betrekking heeft op de persoonsgegevens die de ombudsman heeft verzameld tot aan de datum van het verzoek. De persoonsgegevens die verwerkt worden om aan het verzoek te kunnen voldoen, maken daarvan dus geen onderdeel uit.

Wijze van behandeling

Een AVG-verzoek wordt schriftelijk behandeld. Daarbij geldt als uitgangspunt dat bij digitaal ingediende verzoeken de informatie – voor zover mogelijk – ook digitaal wordt verstrekt, tenzij de betrokkene anders wenst.



**nationale
ombudsman**

[Verlenging van de wettelijke beslistermijn](#)

Verzoeken worden in beginsel binnen één maand na ontvangst behandeld. Als het gaat om veel verzoeken van dezelfde persoon of complexe verzoeken is verlenging met twee maanden mogelijk. Als daar gebruik van wordt gemaakt moet de betrokkene hierover binnen een maand na ontvangst van het verzoek worden geïnformeerd.

[Kosteloos](#)

AVG-verzoeken worden in principe kosteloos behandeld. Als kan worden bewezen dat een verzoek kennelijk ongegrond of buitensporig is, mag een redelijke administratieve vergoeding worden gevraagd of mag het verzoek worden geweigerd (art. 12 lid 5 AVG).

4 Proces in detail

Niet alle rechten van betrokkenen kunnen zijn van toepassing op de verwerkingen van de ombudsman. In onderstaande tabel staat een overzicht waarin de toepasbaarheid van rechten bij grondslagen wordt weergegeven (bron: [Respecteer de rechten van individuen | European Data Protection Board](#)).

		Rechtsgrondslag					
		Toestemming	Overeenkomst	Wettelijke verplichting ²	Vitale belangen	Publiek belang ²	Gerechtvaardigd belang
Rechten van de betrokkene	Gegevens	✓	✓	✓	✓	✓	✓
	Toegang	✓	✓	✓	✓	✓	✓
	Rectificatie	✓	✓	✓	✓	✓	✓
	Verwijdering	✓	✓	✗ Niet van toepassing ¹	✓	✗ Niet van toepassing	✓
	Beperking van de verwerking	✓	✓	✓	✓	✓	✓
	Overdraagbaarheid	✓	✓	✗ Niet van toepassing	✗ Niet van toepassing	✗ Niet van toepassing	✗ Niet van toepassing
	Bezwaar	✗ Niet van toepassing: Je moet je toestemming trekken	✗ Niet van toepassing	✗ Niet van toepassing	✗ Niet van toepassing	✓	✓ Te allen tijde voor Direct Marketing
	Geen volledig geautomatiseerd besluit incl. profilering	Recht op menselijke tussenkomst	Recht op menselijke tussenkomst	Recht op menselijke tussenkomst	✓	✓	✓



DATA PROTECTION GUIDE
FOR SMALL BUSINESS

¹ Om verwijdering kan worden verzocht als de persoonsgegevens moeten worden verwijderd om te voldoen aan een wettelijke verplichting.

² De verwerkingsgrondslag moet worden vastgelegd in de wetgeving van de Unie of de lidstaten.

Binnenkomst AVG-verzoek

Een AVG-verzoek van een betrokkene kan via verschillende kanalen worden ontvangen. Op de website worden betrokkenen verzocht een verzoek per post of per email in te dienen:

Nationale ombudsman
T.a.v. de functionaris voor de gegevensbescherming
Postbus 93122
2509 AC Den Haag

avg@nationaleombudsman.nl

Een verzoek kan ook via een andere weg of bij een andere medewerker binnenkomen. Bijvoorbeeld via een brief of e-mail in een verzoekdossier. De behandelaar van het verzoekdossier brengt zo snel mogelijk de Privacy Officer op de hoogte van het AVG-verzoek, zodat deze in behandeling kan worden genomen.

Bij telefonisch ingediende verzoeken, verzoeken we indiener om het verzoek schriftelijk in te dienen.

Verzoek afkomstig van betrokkene

Betrokkene kan slechts een verzoek indienen voor zover het betrekking heeft op zijn/haar eigen gegevens of voor een kind jonger dan 16 jaar. Dit laatste kan alleen als de aanvrager wettelijk vertegenwoordiger is van het kind. Dit betekent dat de betrokkene gezag heeft over het kind.

Vertegenwoordiger

Een verzoek kan worden ingediend door een vertegenwoordiger van de betrokkene, bijvoorbeeld een voogd/ouder namens een minderjarig kind of een advocaat namens een cliënt. Om te borgen dat het verzoek daadwerkelijk voor de betrokkene is ingediend, moet de vertegenwoordiger aantonen dat hij/zij bevoegd is de betrokkene te vertegenwoordigen, door een machtiging te overleggen.

Minderjarigen

Een ouder kan de rechten uit de AVG van zijn/haar kind uitoefenen als die ouder de wettelijke vertegenwoordiger is. Dat is het geval wanneer die ouder het gezag over het kind heeft. Als eraan wordt getwijfeld of de ouder het gezag heeft, kan de ouder gevraagd worden om een recent uittreksel uit het gezagsregister te overleggen.

Vreemde talen

Een verzoek kan alleen worden gedaan in de Nederlandse, Engelse, Franse of Duitse taal. We reageren altijd in het Nederlands met daarbij een brief in het Engels, Frans of Duits waarin staat dat betrokkene zelf voor vertaling moet zorgen.

Verzoek om informatie o.g.v. de Woo

De Wet open overheid (Woo) is van toepassing op de Nationale ombudsman. De Woo is bedoeld om informatie vastgelegd in documenten op te vragen. De Woo biedt niet het juiste juridische kader om persoonsgegevens op te vragen. Andersom is de AVG niet het juiste juridische kader om informatie vastgelegd in documenten op te vragen. Als er onduidelijkheid bestaat over of een inzageverzoek een Woo-verzoek of AVG-verzoek is, overleggen de PO en de Woo-coördinator hierover. Zo nodig wordt de indiener om nadere informatie gevraagd, zie 4.5 'specificatie verzoek'.

Als duidelijk wordt dat een inzageverzoek een Woo-verzoek betreft, verwijst de PO de indiener naar de Woo-coördinator. Een Woo-verzoek kan worden ingediend via woo@nationaleombudsman.nl.

4.1 Registratie van AVG-verzoek in Djuma

Nadat de PO bepaald heeft dat het om een AVG-verzoek gaat, wordt een dossier aangemaakt in Djuma met het zaaktype 'AVG'.

In Djuma

AVG-zaak wordt aangemaakt met in de omschrijving een beschrijving van het type AVG-verzoek en de startdatum op datum ontvangst van het verzoek.

4.2 Uitvoeren van controles

Voordat een AVG-verzoek in behandeling wordt genomen, wordt door de PO een aantal controles uitgevoerd.

4.2.1 Controle identiteit

Wij vragen niet standaard aan een indiener om zich te legitimeren door overlegging van zijn/haar legitimatiebewijs. Dit doen we alleen in die gevallen waarin we na de volgende stappen twijfels hebben over de identiteit van degene die het AVG-verzoek indient.

Ga na of de indiener en/of intermediair al bij ons bekend is.

Belt iemand in een lopende zaak overtuig jezelf er dan van dat je met de indiener of intermediair zelf te maken hebt.

Stel zo nodig één of meer controlerende vragen; vraag bijvoorbeeld naar het dossiernummer of de adresgegevens.

Indien er twijfel is over de identiteit van de indiener en deze niet naar tevredenheid kan worden vastgesteld kan gevraagd worden aan betrokkene om zich te legitimeren. De indiener kan zich legitimeren door middel van het versturen van een kopie van het legitimatiebewijs.

De vraag om legitimatie kan worden meegenomen in de ontvangstbevestiging, zie 4.4 'versturen ontvangstbevestiging'.

Als de identiteit eenmaal is vastgesteld moet een kopie van een legitimatiebewijs direct worden verwijderd, de kopie wordt niet opgeslagen. In de Djuma-zaak wordt geregistreerd dat de identiteit is vastgesteld.

In Djuma

Indien identiteit is vastgesteld in het veld 'Toelichting' de tekst 'identiteit vastgesteld op <dd-mm-yyyy> met behulp van <type id>'.

4.2.2 Controle veelvragers

Als de betrokkene buitensporig veel AVG-verzoeken doet hoeven we daar geen gehoor aan te geven. De PO controleert of de betrokkene een veelvrager is aan de hand van het bestaan van eerdere verzoeken in Djuma. Betreft het een veelvrager dan wordt de betrokkene per brief (post of digitaal) op de hoogte gebracht van het besluit een verzoek niet in behandeling te nemen. Zie bijlage B, 'Besluit afwijzing AVG-verzoek', 'Tekst 1: Geen gevolg geven aan het verzoek'.

4.3 Versturen ontvangstbevestiging

Na binnenkomst van een inzageverzoek verstuurt de PO de indiener een ontvangstbevestiging. Hiervoor kan Tekst 1: 'Standaard ontvangstbevestiging' uit Bijlage B worden gebruikt.

Als een indiener zich (nog) niet naar tevredenheid heeft weten te identificeren kan hier in de ontvangstbevestiging om gevraagd worden. Zie hiervoor Tekst 2: 'Aanvulling op ontvangstbevestiging indien identificatie nog niet is vastgesteld' uit Bijlage B. In deze tekst wordt ook verwezen naar een website van de rijksoverheid waar staat hoe een veilige kopie van een ID gemaakt kan worden.

Wanneer de gevraagde benodigde informatie uitblijft, wordt nog éénmaal om de vereiste informatie verzocht. Blijft de informatie dan nog uit dan wordt de indiener schriftelijk op de hoogte gesteld dat het AVG-verzoek niet in behandeling kan worden genomen, met opgave van reden. Zie bijlage B, 'besluit afwijzing AVG-verzoek', Tekst 1: 'Geen gevolg geven aan het verzoek'.

4.4 Specificatie verzoek

Als het verzoek van de betrokkene algemeen van aard is (een vraag om alle geregistreerde persoonsgegevens) of er blijkt onvoldoende informatie voorhanden om adequaat op het verzoek te reageren, kan om nadere informatie of specificering van het verzoek gevraagd worden. Denk hierbij bijvoorbeeld aan:

- De duiding van het verzoek
- De hoedanigheid van de betrokkene (advocaat, journalist, leverancier, etc.)
- Specifieke gegevens die gevraagd worden, etc.

4.5 Geen gevolg geven aan het verzoek/het verzoek wordt beperkt

Slechts in uitzonderlijke situaties kan in zijn geheel of beperkt geen gevolg worden gegeven aan een verzoek.

Dit is bijvoorbeeld mogelijk als de betrokkene zich op ons verzoek niet identificeert (art. 11 lid 2 AVG). Het 'niet kunnen vinden' van gegevens kan nooit als grond worden aangevoerd. Wanneer geen gevolg aan het verzoek gegeven kan worden, moet de betrokkene daarvan op de hoogte worden gebracht. Dit moet worden gemotiveerd, waarbij ook moet worden gewezen op de mogelijkheid een klacht in te dienen bij de Autoriteit Persoonsgegevens (art. 12 lid 4 AVG).

Beperking van een verzoek is mogelijk als dat op grond van een Europese of nationale wet is voorgeschreven. Voorwaarde is wel dat de beperking niet in strijd is met de inhoud van grondrechten en fundamentele vrijheden en de beperking een noodzakelijke en evenredige maatregel is (art. 23 AVG). Bij verzoeken die betrekking hebben op het primaire proces is eerder dan bij verzoeken over de bedrijfsvoering te verwachten dat aanleiding bestaat het

verzoek niet in te willigen of te beperken.

Redenen om geen gevolg te geven aan een verzoek

De AVG is niet van toepassing omdat:

Art. 2 lid 2 sub d AVG:

De gegevens worden verwerkt met het oog op voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten.

De gegevens worden verwerkt met het oog op de tenuitvoerlegging van strafrechtelijke sancties.

De gegevens worden verwerkt in het kader van de bescherming tegen en voorkoming van gevaren openbare veiligheid/nationale veiligheid.

Art. 11 lid 2 juncto art. 12 lid 2 AVG

Nadat aanvullende gegevens zijn gevraagd, is identificatie nog steeds niet mogelijk.

Art. 12 lid 5 AVG

Het verzoek is buitensporig (repetitief).

Gebruik bij deze redenen de tekst in Bijlage B, 'Besluit afwijzing AVG-verzoek', Tekst 1: 'Geen gevolg geven aan het verzoek'.

Redenen om het verzoek te beperken

Art. 23 AVG

Een wettelijke grondslag maakt beperking van het verzoek mogelijk, mits die beperking de grondrechten en fundamentele vrijheden onverlet laat en een noodzakelijke en evenredige maatregel is ter waarborging van:

- a. De nationale veiligheid;
- b. Landsverdediging;
- c. Openbare veiligheid;
- d. Voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, incl. bescherming en voorkoming van gevaren voor openbare veiligheid;
- e. Doelstellingen van de EU of van een lidstaat (economisch/financieel, monetair, budgettair, fiscaal, volksgezondheid en sociale zekerheid);
- f. Bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
- g. De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van beroepsregels voor gereguleerde beroepen;
- h. Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van openbaar gezag in de bovengenoemde gevallen (m.u.v. punt f.);
- i. Bescherming van betrokkene of rechten en vrijheden van anderen;
- j. Inning van civielrechtelijke vorderingen

Gebruik bij deze redenen de tekst in Bijlage B, Besluit afwijzing AVG-verzoek, Tekst 2: 'Beperking van het verzoek'.

Hierna wordt de inhoudelijke behandeling van AVG-verzoeken uiteengezet. Er wordt voor de behandeling een onderscheid gemaakt tussen inzageverzoeken en overige AVG-verzoeken.

4.6 Behandeling AVG-verzoek

Als de belangrijkste controles zijn uitgevoerd en de ontvangstbevestiging verzonden is, start de PO met de behandeling van het AVG-verzoek.

4.6.1 Inzageverzoeken

4.6.1.1 Verzamelen van persoonsgegevens

Artikel 15 AVG geeft de betrokkene het recht op een kopie van persoonsgegevens. Dit geeft de betrokkene niet het recht op een volledige kopie van de documenten¹. In sommige gevallen kan volstaan worden met inzicht te geven in de geregistreerde NAW-gegevens van de betrokkene en/of een Excel lijst met een opsomming van stukken en de persoonsgegevens die daarin zijn vastgelegd. Het kan nodig zijn om een kopie van de stukken te verstrekken om de betrokkene in staat te stellen de rechtmatigheid en nauwkeurigheid van de verwerkte gegevens te kunnen controleren².

De PO maakt altijd een afweging of een overzicht met kopie van de persoonsgegevens volstaat om aan het inzagerecht te voldoen.

Het inzagerecht strekt zich niet uit tot interne notities die de persoonlijke gedachten van medewerkers bevatten en die uitsluitend bedoeld zijn voor intern overleg en beraad.

Betrokken medewerkers

De PO bepaalt aan de hand van de reikwijdte van het inzageverzoek en de informatiesystemen welke medewerkers betrokken zijn bij het verzamelen van persoonsgegevens. Vaak is dit de behandelaar van de betreffende zaak.

PO vraagt aan de behandelaar van (gearchiveerde) klachtzaak of alle documenten (op G-schijf, e-mails, appberichten, enz.) in het dossier zitten.

Zo niet, dan dient behandelaar de documenten naar het Serviceteam (ST) te sturen. Het ST zal de documenten aan de gearchiveerde zaak toevoegen.

Reikwijdte inzageverzoek

Alle persoonsgegevens die door betrokkene worden opgevraagd, waaronder persoonsgegevens in bestanden (digitaal of papier);

NAW-gegevens uit Djuma;

Volgstukken uit Djuma (eventueel ook de stukken die de betrokkene zelf heeft aangeleverd als daarom gevraagd wordt);

- Stukken op de G-schijf;
- E-mailberichten in Outlook;
- Overige systemen en opbergkasten;

¹ HvJ EU 20 april 2023, ECLI:EU:C:2023:315 (Conclusie A-G Emiliou)

² HVJ EU 4 mei 2023, ECLI:EU:C:2023:369, JBP 2023/102

- Interne notities (aantekeningen, correspondentie binnen de ombudsman) wat gedeeld is met meer dan één persoon, vallen onder de reikwijdte van een verzoek.

Anonimiseren, indien stukken worden verstrekt

Als er door het inzageverzoek ook persoonsgegevens van andere betrokkenen (derden) ingezien kunnen worden, bepaalt de PO of het delen van die informatie de privacy van anderen schaadt. Is dat het geval, dan dienen de persoonsgegevens geanonimiseerd te worden. Dit kan met behulp van de anonimiseringstool ('Anonimiseren'). Zie voor een werkinstructie de ['handleiding Datamask voor gebruikers'](#).

Bij twijfel, of als anonimiseren te veel werk met zich meeneemt kan contact worden gezocht met de derden om te horen of er bezwaren zijn tegen het delen van de persoonsgegevens.

Aanleveren op centraal punt

De PO maakt een map op de G-schijf beschikbaar waar alle geprepareerde informatie centraal wordt verzameld om te versturen naar de indiener.

4.6.1.2 Antwoord (inhoudelijk) op het verzoek

Bij de beantwoording van een inzageverzoek wordt zoveel mogelijk gebruik gemaakt van standaard teksten en brieven.

In principe vindt beantwoording digitaal (via e-mail) plaats, tenzij de indiener expliciet om communicatie per post vraagt of het verzoek ook via de post heeft ingediend.

Indien stukken gedeeld worden met de indiener, worden deze aan indiener aangeboden via een beveiligd uitwisselingsplatform als Secure Transfer.

Geen persoonsgegevens

Het kan zijn dat de ombudsman geen persoonsgegevens verwerkt van de betrokkene. In dat geval laat de PO de betrokkene weten dat hij/zij niet bekend is bij de ombudsman en dat er geen persoonsgegevens van hem/haar zijn verwerkt. Zie Bijlage B, 'Antwoorden op het verzoek', Tekst 1: 'Geen persoonsgegevens aanwezig'.

Verzoek inwilligen

Het verzoek wordt ingewilligd, als geen bezwaren bestaan op grond waarvan aan het verzoek van de betrokkene geen gevolg zou moeten worden gegeven of het verzoek beperkt zou moeten worden.

De beantwoording op een AVG-inzageverzoek bestaat uit drie delen:

1. Een begeleidende brief

Deze brief, ondertekend door de FG, bevat de reactie op het verzoek. Hierin wordt aangegeven in welke type verwerkingen persoonsgegevens zijn teruggevonden. De brief geeft ook aan welke stappen de betrokkene kan ondernemen als hij/zij niet tevreden is met de afhandeling. Tot slot bevat de brief contactgegevens van de PO.

2. Een bijlage

De bijlage is één document en bestaat uit een aantal delen:

Hoe gaan we om met uw persoonsgegevens

Hier wordt uitgelegd hoe persoonsgegevens worden gebruikt bij de ombudsman. Deze tekst komt grotendeels uit de privacyverklaring van de website.

Overzicht van typen verwerkingen

Een opsomming in tabelvorm van de typen verwerking waar de persoonsgegevens van de betrokkene zijn geregistreerd. De gegevens van de verwerkingen komen uit het verwerkingsregister en tonen tenminste:

De doelen waarvoor we de persoonsgegevens verwerken;

De categorieën persoonsgegevens die we verwerken;

De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of worden doorgegeven;

Hoe lang we de gegevens bewaren of de criteria om de bewaartermijn te bepalen;

Of er sprake is van doorgifte buiten de EER;

Of er sprake is van geautomatiseerde besluitvorming;

Wanneer de persoonsgegevens niet bij de betrokkene zelf zijn verzameld, alle beschikbare informatie over de bron van de gegevens.

Overzicht NAW-gegevens in Djuma

Een opsomming in tabelvorm van de NAW-gegevens die van de betrokkene zijn vastgelegd in Djuma.

Overzicht dossiers

Een opsomming in tabelvorm van alle gevonden dossiers, het type dossier en een korte omschrijving van de dossiers.

3. Een versleutelde map met de persoonsgegevens

De verzamelde persoonsgegevens worden via een beveiligd uitwisselingsplatform (Secure Transfer) verstuurd. Hiervoor is een e-mailadres en telefoonnummer van indiener nodig. De indiener ontvangt via e-mail bericht dat er een gegevens klaar staan om te downloaden. Via een SMS bericht krijgt de indiener een code waarmee de gegevens kunnen worden gedownload.

Als er geen telefoonnummer van indiener bekend is, kan dit worden opgevraagd om de kopie van persoonsgegevens te kunnen versturen via een beveiligde manier. Indien indiener geen telefoonnummer wil verstrekken, wordt de informatie per e-mail verstuurd.

Als de indiener om een schriftelijke reactie per post vraagt worden de gevraagde persoonsgegevens geprint en samen met de begeleidende brief en bijlage aangetekend verstuurd.

In Djuma

De begeleidende brief, de bijlage en het e-mailbericht met de beantwoording wordt in Djuma vastgelegd als volgstuk in het AVG-dossier.

4.6.2 Verwijderverzoek

4.6.2.1 Beoordelen verwijderverzoek

De PO beoordeelt of (deels) gevolg moet worden gegeven aan het verzoek. Er kunnen wettelijke verplichtingen gelden waardoor we verplicht zijn persoonsgegevens voor een bepaalde periode te bewaren. De PO consulteert de archivaris hierover bij onduidelijkheid over de toepasselijke bewaartermijn(en).

De ombudsman is op grond van de Archiefwet verplicht om gegevens te bewaren volgens vastgestelde bewaartermijnen die zijn opgenomen in selectielijsten. Als de gegevens rechtmatig zijn verwerkt kunnen deze niet eerder worden verwijderd dan de vastgestelde bewaartermijn.

In deze situaties geldt het recht op verwijderen:

- De persoonsgegevens zijn niet meer nodig voor het doel waarvoor de gegevens zijn verzameld of waarvoor de gegevens worden verwerkt.
- De persoon in kwestie heeft eerder toestemming gegeven voor het gebruik van de gegevens, maar trekt die toestemming nu in.
- De persoon maakt (terecht) bezwaar tegen het gebruik van de gegevens.
- De organisatie houdt zich niet aan de privacyregels bij het gebruik van de persoonsgegevens. Bijvoorbeeld omdat er geen wettelijke grondslag is voor de verwerking.
- De organisatie is wettelijk verplicht om de gegevens na een bepaalde tijd te verwijderen.
- Apps en websites bij kinderen: de persoonsgegevens van een kind onder de 16 jaar zijn verzameld via een app of website.

In deze situaties geldt het recht op gegevens verwijderen niet:

- De verwerking van de gegevens is noodzakelijk om het recht op vrijheid van meningsuiting en informatie uit te oefenen. Daarmee doet de AVG recht aan het principe dat 'privacy' en 'vrijheid van meningsuiting' gelijkwaardige grondrechten zijn.
- De organisatie verwerkt de gegevens omdat er een wettelijke verplichting is om dat te doen.

- De organisatie verwerkt de gegevens om openbaar gezag of een (wettelijk vastgelegde) taak van algemeen belang uit te oefenen.
- De organisatie verwerkt de gegevens voor een taak van algemeen belang op het gebied van de volksgezondheid.
- De organisatie moet de gegevens in het algemeen belang archiveren.
- De gegevens zijn noodzakelijk voor een rechtsvordering.

4.6.2.2 Inwilligen verwijderverzoek

Het verzoek wordt ingewilligd, als er sprake is van een situatie waarbij het recht op verwijderen geldt.

De PO draagt zorg dat het verzoek wordt uitgevoerd en de betreffende gegevens worden vernietigd. De PO betreft zo nodig medewerkers die bevoegd zijn om de gegevens te vernietigen, bijvoorbeeld om het betreffende dossier te vernietigen.

Daarnaast verzoekt de PO aan betrokken medewerkers, zoals de behandelaar van een klachtdossier, om eventuele stukken met persoonsgegevens op andere plekken (G-schijf, outlook, etc.) te vernietigen.

4.6.2.3 Verzoek beantwoorden

De PO informeert de indiener wat er met het verzoek wordt gedaan. De beantwoording op een AVG-verzoek bestaat uit schriftelijk antwoord per e-mail of per brief.

Als niet kan worden voldaan aan het verzoek kan hiervoor tekst 3: 'AVG-recht niet van toepassing' uit Bijlage 1 worden gebruikt.

Als kan worden voldaan aan het verzoek kan hiervoor tekst 4 'AVG-recht van toepassing' uit Bijlage 1 worden gebruikt.

Informerende andere organisaties

De PO informeert andere organisaties aan wie de persoonsgegevens zijn versterkt, als gevolg wordt gegevens aan het recht op rectificatie, verwijdering, beperking van de verwerking of bezwaar.

In Djuma

Het e-mailbericht met de beantwoording en eventueel de begeleidende brief wordt in Djuma vastgelegd als volgstuk in het AVG-dossier.

4.6.3 Verzoek tot rectificatie

4.6.3.1 Beoordelen verzoek tot rectificatie

De PO beoordeelt of (deels) aan het verzoek tot rectificatie kan worden voldaan of niet.

Een betrokkene kan om rectificatie vragen in een van de volgende situaties:

- De persoonsgegevens kloppen niet;
- De persoonsgegevens zijn niet compleet.

Recht op rectificatie geldt niet als een betrokkene het niet eens is met een indruk, mening of conclusie van of inhoudelijke beoordeling door een medewerker. Feitelijke persoonsgegevens, zoals NAW-gegevens kunnen worden gerectificeerd. Mening en verslagleggingen niet.

Een verzoeker kan wel altijd vragen aan de behandelaar van het verzoekdossier om een toevoeging te doen aan het dossier.

4.6.3.2 Inwilligen verzoek tot rectificatie

Het verzoek wordt ingewilligd, als sprake is van een situatie waarbij het recht op rectificatie van toepassing is.

De PO draagt zorg dat het verzoek wordt uitgevoerd en kan hiervoor een actie uitzetten bij andere medewerkers, bijvoorbeeld medewerkers die bevoegd zijn om NAW-gegevens aan te passen in het systeem.

4.6.3.3 Verzoek beantwoorden

Zie voor de beantwoording [4.6.2.3](#)

4.6.4 Verzoek tot bezwaar

4.6.4.1 Beoordelen verzoek tot bezwaar

De PO beoordeelt of (deels) aan het verzoek moet worden voldaan of niet. Het recht op bewaar kan alleen worden ingezet bij bijzondere persoonlijke omstandigheden.

Het recht op bezwaar geldt alleen als:

- De gegevens worden verwerkt voor een taak van algemeen belang of uitoefening van openbaar gezag;
- De gegevens worden verwerkt op basis van gerechtvaardigd belang; of
- De gegevens worden gebruikt voor profilering.

Als aan bovenstaande voorwaarden is voldaan dan moet de verwerking van de persoonsgegevens opnieuw worden bekeken en een afweging worden gemaakt. De PO doet dit in samenspraak met de FG. De gegevensverwerking moet worden gestopt tenzij er heel goede redenen zijn om de gegevens te blijven verwerken, die zwaarder wegen dan de belangen van de betrokkene.

4.6.4.2 Inwilligen verzoek tot bezwaar

Het verzoek wordt ingewilligd, als sprake is van een situatie waarbij het recht op bezwaar geldt en uit de afweging blijkt dat de gegevensverwerking moet worden gestopt.

De PO draagt zorg dat het verzoek wordt uitgevoerd en de betreffende gegevens worden vernietigd. De PO kan hiervoor een actie uitzetten bij andere medewerkers, bijvoorbeeld medewerkers die bevoegd zijn om dossiers te vernietigen in het zaakstelsel.

4.6.4.3 Verzoek beantwoorden

Zie voor de beantwoording [4.6.2.3](#)

4.6.5 Verzoek tot beperking

4.6.5.1 Beoordelen verzoek tot beperking

De PO beoordeelt of (deels) aan het verzoek kan worden voldaan of niet. Beperking van de verwerking is mogelijk in de volgende situaties:

- De persoonsgegevens zijn mogelijk onjuist (en de betrokkene heeft een rectificatieverzoek ingediend);
- De verwerking van de gegevens is onrechtmatig (maar de betrokkene wil niet dat de gegevens worden verwijderd);
- De gegevens zijn niet meer nodig (maar de betrokkene wil niet dat de gegevens worden verwijderd, omdat die de gegevens nog nodig heeft voor een rechtsvordering);
- De betrokkene heeft bezwaar gemaakt tegen de verwerking van de gegevens vanwege de specifieke situatie van deze persoon (en het is nog niet duidelijk welk belang zwaarder weegt).

Indien niet aan een van bovenstaande voorwaarden is voldaan kan geen gevolg worden gegeven aan het verzoek.

4.6.5.2 Inwilligen verzoek tot beperking

Het verzoek wordt ingewilligd, als sprake is van een situatie waarbij het recht op beperking geldt.

De PO draagt zorg dat het verzoek wordt uitgevoerd en de betreffende gegevens niet worden gebruikt zolang het recht op beperking geldt. Het kan nodig zijn dat de toegang tot een dossier wordt beperkt om te voorkomen dat persoonsgegevens worden gebruikt.

4.6.5.3 Verzoek beantwoorden

Zie voor de beantwoording [4.6.2.3](#)

4.6.6 Verzoek tot overdraagbaarheid (dataportabiliteit)

4.6.6.1 Beoordelen verzoek tot overdraagbaarheid

De PO beoordeelt of (deels) aan het verzoek kan worden voldaan of niet. Alleen gegevens die digitaal zijn vallen onder het recht op dataportabiliteit. Daarnaast geldt het recht alleen voor persoonsgegevens die worden verwerkt met iemands toestemming of als de gegevens nodig zijn om een overeenkomst met diegene uit te voeren.

Indien niet aan de voorwaarden is voldaan kan geen gevolg worden gegeven aan het verzoek.

4.6.6.2 Inwilligen verzoek tot overdraagbaarheid

Het verzoek wordt ingewilligd, als sprake is van een situatie waarbij het recht op overdraagbaarheid van toepassing is.

De PO draagt zorg dat het verzoek wordt uitgevoerd. Alle persoonsgegevens die de betrokkene aan ons heeft verstrekt, moeten beschikbaar worden gesteld. De gegevens moeten worden verstrekt in een gestructureerde, veelgebruikte en machineleesbaar formaat.

4.6.6.3 Verzoek beantwoorden

Zie voor de beantwoording [4.6.2.3](#)

4.6.7 [Recht om niet onderworpen te zijn aan geautomatiseerde besluitvorming](#)

De ombudsman maakt bij de verwerking van persoonsgegevens geen gebruik van geautomatiseerde besluitvorming.

Bijlage A Begrippenlijst

Begrip	Toelichting
PO	De Privacy Officer is verantwoordelijk voor de operationele uitvoering van taken die voortvloeien uit de AVG.
AVG-vertegenwoordiger	Een medewerker van een team of domein die als aanspreekpunt fungeert voor AVG vragen.
Indiener	Dit is degene die feitelijk het inzageverzoek indient. In de meeste gevallen is de indiener ook de betrokkene. De indiener kan een burger maar ook een wettelijk vertegenwoordiger, bewindvoerder, gemachtigde of intermediair zijn.
Betrokkene	Dit is een natuurlijk persoon die op basis van persoonsgegevens direct of indirect kan worden geïdentificeerd.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (tekst afkomstig uit AVG).
Veelvrager	Dit is een indiener of betrokkene die buitensporig veel inzageverzoeken indient.
Derde	Dit is een natuurlijk persoon van wie zijn persoonsgegevens bij het verzamelen van een inzageverzoek naast die van de betrokkene ook inzichtelijk zijn geworden, maar waarvan deze gegevens niet er inzage gegeven/verstrekt worden aan de betrokkene.

Bijlage B Modelteksten

Ontvangstbevestiging

Tekst 1: Standaard ontvangstbevestiging.

Geachte <naam betrokkene>,

De Ombudsman heeft op <datum> uw verzoek op basis van de AVG van <datum> ontvangen. Uw verzoek wordt in behandeling genomen en u verneemt zo snel mogelijk, uiterlijk binnen vier weken, nader bericht.

Indien uw verzoek complex van aard of veel omvattend blijkt te zijn is het mogelijk dat de reactietermijn verlengd wordt met maximaal twee maanden. U wordt daarvan binnen één maand op de hoogte gebracht.

Met vriendelijke groet,

<ondertekening PO>

Tekst 2: Aanvulling op ontvangstbevestiging indien identificatie nog niet is vastgesteld.

Om uw identiteit deugdelijk vast te kunnen stellen hebben we aanvullende informatie nodig. Ter bevestiging van uw identiteit verzoek ik u mij zo spoedig mogelijk een kopie van een geldig identiteitsbewijs te sturen.

Hoe u een veilige kopie maakt vindt u hier:

<https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/veilige-kopie-identiteitsbewijs?>

De kopie van uw identiteitsbewijs wordt direct vernietigd zodra uw identiteit is vastgesteld.

Besluit geen gevolg/beperking AVG-verzoek

Tekst 1: Geen gevolg geven aan het verzoek

Geachte <naam betrokkene>,

Naar aanleiding van uw AVG-verzoek van <datum verzoek> bericht ik u als volgt.
Er wordt geen gevolg gegeven aan uw verzoek, omdat <reden afwijzing>.

Als u niet tevreden bent met de wijze waarop uw verzoek is afgehandeld, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

Tekst 2: Beperking van het verzoek

Geachte <naam betrokkene>,

Naar aanleiding van uw AVG-verzoek van <datum verzoek> bericht ik u als volgt. Er is een wettelijke grondslag die maakt dat uw verzoek wordt beperkt. Beperking van uw verzoek is een noodzakelijke en evenredige maatregel ter waarborging van <reden genoemd in art. 23 sub a t/m j AVG>.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

[Antwoorden op het AVG-verzoek](#)

Tekst 1: Geen persoonsgegevens aanwezig

Geachte <naam betrokkene>,

Naar aanleiding van uw verzoek van <datum verzoek> bericht ik u als volgt. U bent bij de Nationale ombudsman niet bekend. Er worden geen persoonsgegevens van u door de Nationale ombudsman verwerkt.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

Tekst 2: Verstrekken kopie persoonsgegevens

Geachte <naam betrokkene>,

In de bijgevoegde brief treft u het antwoord van de Nationale ombudsman aan op uw AVG-verzoek om inzage in uw persoonsgegevens.

U ontvangt apart een e-mailbericht met een Secure Transfer link naar [een Excel bestand met daarin een overzicht van de gevraagde persoonsgegevens/de afschriften van de stukken waarin uw persoonsgegevens zijn opgenomen].

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

Tekst 3: AVG-recht niet van toepassing

Geachte <naam betrokkene>,

Naar aanleiding van uw verzoek van <datum verzoek> bericht ik u als volgt.

U verzoekt om <AVG-recht> met betrekking tot dossier met zaaknummer <nummer>. Het recht op <AVG-recht> geldt alleen in bepaalde situaties. Zie voor meer informatie de website van de Autoriteit Persoonsgegevens <link>.

Het recht op <AVG-recht> is hier niet van toepassing.

Als u niet tevreden bent met de wijze waarop uw verzoek is afgehandeld, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

Tekst 4: AVG-recht van toepassing

Geachte <naam betrokkene>,

Naar aanleiding van uw verzoek van <datum verzoek> bericht ik u als volgt.

U verzoekt om <AVG-recht> met betrekking tot dossier met zaaknummer <nummer>. Het recht op <AVG-recht> is hier van toepassing.

Als u niet tevreden bent met de wijze waarop uw verzoek is afgehandeld, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>



AVG-VERZOEKEN

Procesbeschrijving

1	INLEIDING.....	2
2	RECHTEN VAN BETROKKENEN	3
3	AANDACHTSPUNTEN.....	4
4	PROCES IN DETAIL.....	6
4.1	BINNENKOMST AVG-VERZOEK.....	6
4.2	REGISTRATIE VAN INZAGEVERZOEK IN DJUMA	8
4.3	UITVOEREN VAN CONTROLES	8
4.3.1	<i>Controle identiteit</i>	8
4.3.2	<i>Controle veelvragers.....</i>	8
4.4	VERSTUREN ONTVANGSTBEVESTIGING	9
4.5	SPECIFICATIE VERZOEK.....	9
4.6	GEEN GEVOLG GEVEN AAN HET VERZOEK/HET VERZOEK WORDT BEPERKT.....	9
4.7	BEHANDELING INZAGEVERZOEK	11
4.7.1	<i>Verzamelen van persoonsgegevens.....</i>	11
4.7.2	<i>Antwoord (inhoudelijk) op het verzoek.....</i>	12
4.7.2.1	<i>Geen persoonsgegevens</i>	12
4.7.2.2	<i>Verzoek inwilligen</i>	12
4.8	BEHANDELING AVG-VERZOEK	14
4.8.1	<i>Beoordelen verzoek.....</i>	14
	<i>Verwijderverzoek.....</i>	Fout! Bladwijzer niet gedefinieerd.
	<i>Verzoek tot rectificatie</i>	15
4.9	VERZOEK INWILLIGEN	17
	<i>Informeren andere organisaties</i>	17
4.10	BEANTWOORDING AVG-VERZOEK	FOUT! BLADWIJZER NIET GEDEFINIEERD.
	BIJLAGE A BEGRIPPENLIJST	18
	BIJLAGE B MODELTEKSTEN	19
	ONTVANGSTBEVESTIGING	19
	BESLUIT AFWIJZING AVG-VERZOEK.....	20
	ANTWOORDEN OP HET AVG-VERZOEK	21

1 Inleiding

De Algemene Verordening Gegevensbescherming (AVG) is een Europese wet die de privacy rechten van individuen regelt en de manier waarop organisaties persoonsgegevens verwerken.

In artikel 13 t/m 22 staan alle rechten van betrokkene. In het kader van de AVG zijn de betrokkenen degenen van wie persoonsgegevens worden verwerkt. Met betrekking tot de verwerking van hun persoonsgegevens hebben de betrokkenen een aantal rechten onder de AVG. Wanneer iemand gebruik maakt van (een) deze rechten dan spreken we van een verzoek van een betrokkene (in dit document wordt hiervoor de term 'AVG-verzoek' gebruikt).

Afhankelijk van de reikwijdte en complexiteit van een verzoek op basis van genoemde artikelen uit de AVG kan afhandeling hiervan een zeer tijdsintensieve onderneming zijn waarbij een aantal stappen doorlopen moet worden.

Om een verzoek van een betrokkene uniform, efficiënt en binnen de wettelijke reactietermijn te kunnen afhandelen is een duidelijke procesbeschrijving nodig.

Het proces met betrekking tot de rechten van de betrokkene is in dit document beschreven.

Met opmerkingen [MD1]: Ik zou dit tekstgedeelte verplaatsen naar de Inleiding (aanleiding van procesbeschrijving) . Dit tekst gedeelte zegt niets over de rechten van betrokkenen.

2 Rechten van betrokkenen

De AVG kent de volgende rechten van betrokkenen:

- **Recht op informatie** (art. 13 en 14 AVG): Organisaties moeten betrokkenen informeren over de verwerking van hun persoonsgegevens. Dit omvat details zoals de doeleinden van de verwerking, de categorieën van persoonsgegevens die worden verwerkt, en de rechten van de betrokkenen.
- **Recht op inzage** (art. 15 AVG): Betrokkenen hebben het recht om te weten of hun persoonsgegevens worden verwerkt, en zo ja, om deze gegevens in te zien.
- **Recht op rectificatie** (art. 16 AVG): Betrokkenen hebben het recht om onjuiste persoonsgegevens te laten corrigeren en onvolledige gegevens aan te vullen.
- **Recht op gegevenswissing** (art. 17 AVG): Betrokkenen hebben in bepaalde gevallen het recht om hun persoonsgegevens te laten wissen.
- **Recht op beperking van de verwerking** (art. 18 AVG): Betrokkenen hebben onder bepaalde omstandigheden het recht om de verwerking van hun persoonsgegevens te beperken.
- **Recht van overdraagbaarheid (dataportabiliteit)** (art. 20 AVG): Betrokkenen hebben het recht om hun persoonsgegevens te ontvangen in een gestructureerd, veelgebruikt en machine leesbaar formaat, en ze hebben het recht om deze gegevens over te dragen aan een andere verwerkingsverantwoordelijke.
- **Recht van bezwaar** (art. 21 AVG): Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens op basis van bepaalde gronden.
- **Recht om niet onderworpen te zijn aan geautomatiseerde besluitvorming** (art. 22 AVG): Betrokkenen hebben het recht om niet onderworpen te worden aan besluiten die uitsluitend gebaseerd zijn op geautomatiseerde verwerking, inclusief profilering, tenzij dit gerechtvaardigd is en bepaalde voorwaarden zijn vervuld.

3 Aandachtspunten

PDCA-cyclus

Deze procesbeschrijving is onderdeel van de AVG-verbetercyclus. Dit betekent dat het proces periodiek wordt getoetst aan de praktijkervaringen, wijzigingen in wet- en regelgeving en de inrichting van de organisatie.

De Privacy officer (PO) behandelt AVG-verzoeken

Om de uniformiteit van het afhandelen van verzoeken te bewaken en vanwege de korte wettelijke behandeltermijn worden de verzoeken door de PO behandeld.

De FG toetst de behandeling van een AVG-verzoek en ondertekent de begeleidende brief bij beantwoording van een AVG-verzoek.

Registratie in Djuma

AVG-verzoeken worden geregistreerd in Djuma op een uniforme wijze. Hierdoor is eenvoudig te rapporteren over AVG-verzoeken. Voor registratie van AVG-verzoeken wordt het zaaktype 'AVG' gebruikt.

Antimisbruikbepaling

De AVG bevat een antimisbruikbepaling. Dit betekent dat een verwerkingsverantwoordelijke mag weigeren gevolg te geven aan een AVG-verzoek als bedoeld in artikelen 13 t/m 22 als het verzoek kennelijk ongegrond of buitensporig is.

Van kennelijk ongegrond is sprake als er duidelijk niet is voldaan aan de randvoorwaarden voor een verzoek.

Een verzoek is buitensporig als het een disproportionele last legt op de verwerkingsverantwoordelijke, bijvoorbeeld wanneer het te vaak wordt ingediend of zeer omvangrijke verzoeken betreft. Let wel, dat een verzoek duur, arbeidsintensief of complex is, zal geen argument zijn om te weigeren. In geval van weigering moet de verwerkingsverantwoordelijke aantonen dat het verzoek buitensporig of kennelijk ongegrond is.

Peildatum

Als wordt verzocht om informatie over de verwerking van persoonsgegevens of om inzage in de persoonsgegevens, geldt de datum van ontvangst van het verzoek als peildatum. Dat betekent dat het verzoek betrekking heeft op de persoonsgegevens die de ombudsman heeft verzameld tot aan de datum van het verzoek. De persoonsgegevens die verwerkt worden om aan het verzoek te kunnen voldoen, maken daarvan dus geen onderdeel uit.

Wijze van behandeling

Een AVG-verzoek wordt schriftelijk behandeld. Daarbij geldt als uitgangspunt dat bij digitaal ingediende verzoeken de informatie – voor zover mogelijk – ook digitaal wordt verstrekt, tenzij de betrokkene anders wenst.

Verlenging van de wettelijke beslistermijn

Verzoeken worden in beginsel binnen één maand na ontvangst behandeld. Als het gaat om veel verzoeken van dezelfde persoon of complexe verzoeken is verlenging met twee maanden mogelijk. Als daar gebruik van wordt gemaakt moet de betrokkene hierover binnen een maand na ontvangst van het verzoek worden geïnformeerd.

Kosteloos

AVG-verzoeken worden in principe kosteloos behandeld. Als kan worden bewezen dat een verzoek kennelijk ongegrond of buitensporig is, mag een redelijke administratieve vergoeding worden gevraagd of mag het verzoek worden geweigerd (art. 12 lid 5 AVG).

Met opmerkingen [MD2]: Waar is dit op gebaseerd?

Met opmerkingen [SP3R2]: Toegevoegd: art 12 lid 5 AVG.

4 Proces in detail

Niet alle rechten van betrokkenen kunnen zijn van toepassing op de verwerkingen van de ombudsman. In onderstaande tabel staat een overzicht waarin de toepasbaarheid van rechten bij grondslagen wordt weergegeven (bron: [Respecteer de rechten van individuen | European Data Protection Board](#)).

		Rechtsgrondslag					
		Toestemming	Overeenkomst	Wettelijke verplichting ¹	Vitale belangen	Publiek belang ²	Gerechtvaardigd belang
Rechten van de betrokkene	Gegevens	✓	✓	✓	✓	✓	✓
	Toegang	✓	✓	✓	✓	✓	✓
	Rectificatie	✓	✓	✓	✓	✓	✓
	Verwijdering	✓	✓	✗ Niet van toepassing ¹	✓	✗ Niet van toepassing	✓
	Beperking van de verwerking	✓	✓	✓	✓	✓	✓
	Overdraagbaarheid	✓	✓	✗ Niet van toepassing	✗ Niet van toepassing	✗ Niet van toepassing	✗ Niet van toepassing
	Bezwaar	✗ Niet van toepassing: Je moet je toestemming trekken	✗ Niet van toepassing	✗ Niet van toepassing	✗ Niet van toepassing	✓	✓ Te allen tijde voor Direct Marketing
	Geen volledig geautomatiseerd besluit incl. profilering	Recht op menselijke tussenkomst	Recht op menselijke tussenkomst	Recht op menselijke tussenkomst	✓	✓	✓



DATA PROTECTION GUIDE
FOR SMALL BUSINESS

¹ Om verwijdering kan worden verzocht als de persoonsgegevens moeten worden verwijderd om te voldoen aan een wettelijke verplichting.

² De verwerkingsgrondslag moet worden vastgelegd in de wetgeving van de Unie of de lidstaten.

4.1 Binnenkomst AVG-verzoek

Een AVG-verzoek van een betrokkene kan via verschillende kanalen worden ontvangen. Op de website worden betrokkenen verzocht een verzoek per post of per email in te dienen:

Nationale ombudsman

T.a.v. de functionaris voor de gegevensbescherming

Postbus 93122

2509 AC Den Haag

Met opmerkingen [SW4]: Op de website wordt er nog steeds verwezen naar de FG, moet ook aangepast worden.

avq@nationaleombudsman.nl

Een verzoek kan ook via een andere weg of bij een andere medewerker binnenkomen. Bijvoorbeeld via een brief of e-mail in een verzoekdossier. De behandelaar van het verzoekdossier brengt zo snel mogelijk de Privacy Officer op de hoogte van het AVG-verzoek, zodat deze in behandeling kan worden genomen.

Bij telefonisch ingediende verzoeken, verzoeken we indiener om het verzoek schriftelijk in te dienen.

Met opmerkingen [MD5]: Dus ingekomen via de mail
Mondeling kan dus niet.

Verzoek afkomstig van betrokkene

Betrokkene kan slechts een verzoek indienen voor zover het betrekking heeft op zijn/haar eigen gegevens of voor een kind jonger dan 16 jaar. Dit laatste kan alleen als de aanvrager wettelijk vertegenwoordiger is van het kind. Dit betekent dat de betrokkene gezag heeft over het kind.

Vertegenwoordiger

Een verzoek kan worden ingediend door een vertegenwoordiger van de betrokkene, bijvoorbeeld een voogd/ouder namens een minderjarig kind of een advocaat namens een cliënt. Om te borgen dat het verzoek daadwerkelijk voor de betrokkene is ingediend, moet de vertegenwoordiger aantonen dat hij/zij bevoegd is de betrokkene te vertegenwoordigen, door een machtiging te overleggen.

Minderjarigen

Een ouder kan de rechten uit de AVG van zijn/haar kind uitoefenen als die ouder de wettelijke vertegenwoordiger is. Dat is het geval wanneer die ouder het gezag over het kind heeft. Als eraan wordt getwijfeld of de ouder het gezag heeft, kan de ouder gevraagd worden om een recent uittreksel uit het gezagsregister te overleggen.

Vreemde talen

Een verzoek kan alleen worden gedaan in de Nederlandse, Engelse, Franse of Duitse taal. We reageren altijd in het Nederlands met daarbij een brief in het Engels, Frans of Duits waarin staat dat betrokkene zelf voor vertaling moet zorgen.

Verzoek om informatie o.g.v. de Woo

De Wet open overheid (Woo) is van toepassing op de Nationale ombudsman. De Woo is bedoeld om informatie vastgelegd in documenten op te vragen. De Woo biedt niet het juiste juridische kader om persoonsgegevens op te vragen. Andersom is de AVG niet het juiste juridische kader om informatie vastgelegd in documenten op te vragen. Als er onduidelijkheid bestaat over of een inzageverzoek een Woo-verzoek of AVG-verzoek is, overleggen de PO en de Woo-coördinator hierover. Zo nodig wordt de indiener om nadere informatie gevraagd, zie 4.5 'specificatie verzoek'.

Als duidelijk wordt dat een inzageverzoek een Woo-verzoek betreft, verwijst de PO de indiener naar de Woo-coördinator. Een Woo-verzoek kan worden ingediend via woo@nationaleombudsman.nl.

4.2 Registratie van AVG-verzoek in Djuma

Nadat de PO bepaald heeft dat het om een AVG-verzoek gaat, wordt een dossier aangemaakt in Djuma met het zaaktype 'AVG'.

In Djuma

AVG-zaak wordt aangemaakt met in de omschrijving een beschrijving van het type AVG-verzoek en de startdatum op datum ontvangst van het verzoek.

4.3 Uitvoeren van controles

Voordat een AVG-verzoek in behandeling wordt genomen, wordt door de PO een aantal controles uitgevoerd.

4.3.1 Controle identiteit

Wij vragen niet standaard aan een indiener om zich te legitimeren door overlegging van zijn/haar legitimatiebewijs. Dit doen we alleen in die gevallen waarin we na de volgende stappen twijfels hebben over de identiteit van degene die het AVG-verzoek indient.

- Ga na of de indiener en/of intermediair al bij ons bekend is.
- Belt iemand in een lopende zaak overtuig jezelf er dan van dat je met de indiener of intermediair zelf te maken hebt.
- Stel zo nodig één of meer controlerende vragen; vraag bijvoorbeeld naar het dossiernummer of de adresgegevens.

Indien er twijfel is over de identiteit van de indiener en deze niet naar tevredenheid kan worden vastgesteld kan gevraagd worden aan betrokkene om zich te legitimeren. De indiener kan zich legitimeren door middel van het versturen van een kopie van het legitimatiebewijs.

De vraag om legitimatie kan worden meegenomen in de ontvangstbevestiging, zie 4.4 'versturen ontvangstbevestiging'.

Als de identiteit eenmaal is vastgesteld moet een kopie van een legitimatiebewijs direct worden verwijderd, de kopie wordt niet opgeslagen. In de Djuma-zaak wordt geregistreerd dat de identiteit is vastgesteld.

In Djuma

Indien identiteit is vastgesteld in het veld 'Toelichting' de tekst 'identiteit vastgesteld op <dd-mm-yyyy> met behulp van <type id>'.

4.3.2 Controle veelvragers

Als de betrokkene buitensporig veel AVG-verzoeken doet hoeven we daar geen gehoor aan te geven. De PO controleert of de betrokkene een veelvrager is aan de hand van het bestaan van eerdere verzoeken in Djuma. Betreft het een veelvrager dan wordt de betrokkene per brief (post of digitaal) op de hoogte gebracht van het besluit een verzoek niet in behandeling te nemen. Zie bijlage B, 'Besluit afwijzing AVG-verzoek', 'Tekst 1: Geen gevolg geven aan het verzoek'.

4.4 Versturen ontvangstbevestiging

Na binnenkomst van een inzageverzoek verstuurt de PO de indiener een ontvangstbevestiging. Hiervoor kan Tekst 1: 'Standaard ontvangstbevestiging' uit Bijlage B worden gebruikt.

Als een indiener zich (nog) niet naar tevredenheid heeft weten te identificeren kan hier in de ontvangstbevestiging om gevraagd worden. Zie hiervoor Tekst 2: 'Aanvulling op ontvangstbevestiging indien identificatie nog niet is vastgesteld' uit Bijlage B. In deze tekst wordt ook verwezen naar een website van de rijksoverheid waar staat hoe een veilige kopie van een ID gemaakt kan worden.

Wanneer de gevraagde benodigde informatie uitblijft, wordt nog éénmaal om de vereiste informatie verzocht. Blijft de informatie dan nog uit dan wordt de indiener schriftelijk op de hoogte gesteld dat het AVG-verzoek niet in behandeling kan worden genomen, met opgave van reden. Zie bijlage B, 'besluit afwijzing AVG-verzoek', Tekst 1: 'Geen gevolg geven aan het verzoek'.

4.5 Specificatie verzoek

Als het verzoek van de betrokkene algemeen van aard is (een vraag om alle geregistreerde persoonsgegevens) of er blijkt onvoldoende informatie voorhanden om adequaat op het verzoek te reageren, kan om nadere informatie of specificering van het verzoek gevraagd worden. Denk hierbij bijvoorbeeld aan:

- De duiding van het verzoek
- De hoedanigheid van de betrokkene (advocaat, journalist, leverancier, etc.)
- Specifieke gegevens die gevraagd worden, etc.

4.6 Geen gevolg geven aan het verzoek/het verzoek wordt beperkt

Slechts in uitzonderlijke situaties kan in zijn geheel of beperkt geen gevolg worden gegeven aan een verzoek.

Dit is bijvoorbeeld mogelijk als de betrokkene zich op ons verzoek niet identificeert (art. 11 lid 2 AVG). Het 'niet kunnen vinden' van gegevens kan nooit als grond worden aangevoerd. Wanneer geen gevolg aan het verzoek gegeven kan worden, moet de betrokkene daarvan op de hoogte worden gebracht. Dit moet worden gemotiveerd, waarbij ook moet worden gewezen op de mogelijkheid een klacht in te dienen bij de Autoriteit Persoonsgegevens (art. 12 lid 4 AVG).

Beperking van een verzoek is mogelijk als dat op grond van een Europese of nationale wet is voorgeschreven. Voorwaarde is wel dat de beperking niet in strijd is met de inhoud van grondrechten en fundamentele vrijheden en de beperking een noodzakelijke en evenredige maatregel is (art. 23 AVG). Bij verzoeken die betrekking hebben op het primaire proces is eerder dan bij verzoeken over de bedrijfsvoering te verwachten dat aanleiding bestaat het verzoek niet in te willigen of te beperken.

Redenen om geen gevolg te geven aan een verzoek

De AVG is niet van toepassing omdat:

Art. 2 lid 2 sub d AVG:

- De gegevens worden verwerkt met het oog op voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten.
- De gegevens worden verwerkt met het oog op de tenuitvoerlegging van strafrechtelijke sancties.
- De gegevens worden verwerkt in het kader van de bescherming tegen en voorkoming van gevaren openbare veiligheid/nationale veiligheid.

Art. 11 lid 2 juncto art. 12 lid 2 AVG

Nadat aanvullende gegevens zijn gevraagd, is identificatie nog steeds niet mogelijk.

Art. 12 lid 5 AVG

Het verzoek is buitensporig (repetitief).

Gebruik bij deze redenen de tekst in Bijlage B, 'Besluit afwijzing AVG-verzoek', Tekst 1: 'Geen gevolg geven aan het verzoek'.

Redenen om het verzoek te beperken

Art. 23 AVG

Een wettelijke grondslag maakt beperking van het verzoek mogelijk, mits die beperking de grondrechten en fundamentele vrijheden onverlet laat en een noodzakelijke en evenredige maatregel is ter waarborging van:

- a. De nationale veiligheid;
- b. Landsverdediging;
- c. Openbare veiligheid;
- d. Voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, incl. bescherming en voorkoming van gevaren voor openbare veiligheid;
- e. Doelstellingen van de EU of van een lidstaat (economisch/financieel, monetair, budgettair, fiscaal, volksgezondheid en sociale zekerheid);
- f. Bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
- g. De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van beroepsregels voor gereguleerde beroepen;
- h. Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van openbaar gezag in de bovengenoemde gevallen (m.u.v. punt f.);
- i. Bescherming van betrokkene of rechten en vrijheden van anderen;
- j. Inning van civielrechtelijke vorderingen

Gebruik bij deze redenen de tekst in Bijlage B, Besluit afwijzing AVG-verzoek, Tekst 2: 'Beperking van het verzoek'.

Hierna wordt de inhoudelijke behandeling van AVG-verzoeken uiteengezet. Er wordt voor de behandeling een onderscheid gemaakt tussen inzageverzoeken en overige AVG-verzoeken.

4.7 Behandeling inzageverzoek

Als de belangrijkste controles zijn uitgevoerd en de ontvangstbevestiging verzonden is, start de PO met de behandeling van het AVG-inzageverzoek.

4.7.1 Verzamelen van persoonsgegevens

Artikel 15 AVG geeft de betrokkene het recht op een kopie van persoonsgegevens. Dit geeft de betrokkene niet het recht op een volledige kopie van de documenten¹. In sommige gevallen kan volstaan worden met inzicht te geven in de geregistreerde NAW-gegevens van de betrokkene en/of een Excel lijst met een opsomming van stukken en de persoonsgegevens die daarin zijn vastgelegd. Het kan nodig zijn om een kopie van de stukken te verstrekken om de betrokkene in staat te stellen de rechtmatigheid en nauwkeurigheid van de verwerkte gegevens te kunnen controleren².

De PO maakt altijd een afweging of een overzicht met kopie van de persoonsgegevens volstaat om aan het inzagerecht te voldoen.

Het inzagerecht strekt zich niet uit tot interne notities die de persoonlijke gedachten van medewerkers bevatten en die uitsluitend bedoeld zijn voor intern overleg en beraad.

Betrokken medewerkers

De PO bepaalt aan de hand van de reikwijdte van het inzageverzoek en de informatiesystemen welke medewerkers betrokken zijn bij het verzamelen van persoonsgegevens. Vaak is dit de behandelaar van de betreffende zaak.

PO vraagt aan de behandelaar van (gearchiverde) klachtzaak of alle documenten (op G-schijf, e-mails, appberichten, enz.) in het dossier zitten.

Zo niet, dan dient behandelaar de documenten naar het Serviceteam (ST) te sturen. Het ST zal de documenten aan de gearchiverde zaak toevoegen.

Reikwijdte inzageverzoek

- Alle persoonsgegevens die door betrokkene worden opgevraagd, waaronder persoonsgegevens in bestanden (digitaal of papier);
 - o NAW-gegevens uit Djuma;
 - o Volgstukken uit Djuma (eventueel ook de stukken die de betrokkene zelf heeft aangeleverd als daarom gevraagd wordt);
 - o Stukken op de G-schijf;
 - o E-mailberichten in Outlook;
 - o Overige systemen en opbergkasten;
- Interne notities (aantekeningen, correspondentie binnen de ombudsman) wat gedeeld is met meer dan één persoon, vallen onder de reikwijdte van een verzoek.

Anonimiseren, indien stukken worden verstrekt

Als er door het inzageverzoek ook persoonsgegevens van andere betrokkenen (derden) ingezien kunnen worden, bepaalt de PO of het delen van die informatie de privacy van anderen schaadt. Is dat het geval, dan dienen de persoonsgegevens geanonimiseerd te

¹ HvJ EU 20 april 2023, ECLI:EU:C:2023:315 (Conclusie A-G Emiliou)

² HVJ EU 4 mei 2023, ECLI:EU:C:2023:369, JBP 2023/102

worden. Dit kan met behulp van de anonimiseringsstool ('Anonimiseren'). Zie voor een werkinstructie de '[handleiding Datamask voor gebruikers](#)'.

Bij twijfel, of als anonimiseren te veel werk met zich meeneemt kan contact worden gezocht met de derden om te horen of er bezwaren zijn tegen het delen van de persoonsgegevens.

Aanleveren op centraal punt

De PO maakt een map op de G-schijf beschikbaar waar alle geprepareerde informatie centraal wordt verzameld om te versturen naar de indiener.

4.7.2 Antwoord (inhoudelijk) op het verzoek

Bij de beantwoording van een inzageverzoek wordt zoveel mogelijk gebruik gemaakt van standaard teksten en brieven.

In principe vindt beantwoording digitaal (via e-mail) plaats, tenzij de indiener expliciet om communicatie per post vraagt of het verzoek ook via de post heeft ingediend.

Indien stukken gedeeld worden met de indiener, worden deze aan indiener aangeboden via een beveiligd uitwisselingsplatform als Secure Transfer.

4.7.2.1 Geen persoonsgegevens

Het kan zijn dat de ombudsman geen persoonsgegevens verwerkt van de betrokkene. In dat geval laat de PO de betrokkene weten dat hij/zij niet bekend is bij de ombudsman en dat er geen persoonsgegevens van hem/haar zijn verwerkt. Zie Bijlage B, 'Antwoorden op het verzoek', Tekst 1: 'Geen persoonsgegevens aanwezig'.

4.7.2.2 Verzoek inwilligen

Het verzoek wordt ingewilligd, als geen bezwaren bestaan op grond waarvan aan het verzoek van de betrokkene geen gevolg zou moeten worden gegeven of het verzoek beperkt zou moeten worden.

De beantwoording op een AVG-inzageverzoek bestaat uit drie delen:

1. Een begeleidende brief

Deze brief, ondertekend door de FG, bevat de reactie op het verzoek. Hierin wordt aangegeven in welke type verwerkingen persoonsgegevens zijn teruggevonden. De brief geeft ook aan welke stappen de betrokkene kan ondernemen als hij/zij niet tevreden is met de afhandeling. Tot slot bevat de brief contactgegevens van de PO.

2. Een bijlage

De bijlage is één document en bestaat uit een aantal delen:

Hoe gaan we om met uw persoonsgegevens

Hier wordt uitgelegd hoe persoonsgegevens worden gebruikt bij de ombudsman. Deze tekst komt grotendeels uit de privacyverklaring van de website.

Overzicht van typen verwerkingen

Een opsomming in tabelvorm van de typen verwerking waar de persoonsgegevens van de betrokkene zijn geregistreerd. De gegevens van de verwerkingen komen uit het verwerkingsregister en tonen tenminste:

- De doelen waarvoor we de persoonsgegevens verwerken;
- De categorieën persoonsgegevens die we verwerken;
- De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of worden doorgegeven;
- Hoe lang we de gegevens bewaren of de criteria om de bewaartermijn te bepalen;
- Of er sprake is van doorgifte buiten de EER;

Met opmerkingen [MD6]: Kan je niet beter schrijven de anonimiseringsstool (Datamask). De tool heet toch niet Anonimiseren? En het is toch nog steeds van Datamask?

Met opmerkingen [SP7R6]: Aangepast naar anonimiseringsstool. Na de recente overname door xxlnc, heet de tool tegenwoordig Anonimiseren, niet langer Datamask.

Met opmerkingen [MD8R6]: Ik zou (voorheen Datamask) weglaten. Deze benaming is er blijkbaar dus niet meer. In vervolg daarop zou ik in de titel Handleiding Datamask voor gebruikers', Datamask ook vervangen voor de Anonimiseren.

Met opmerkingen [MD9]: Strookt dit met het proces van anonimiseren? Anonimiseren gebeurt toch in Djuma vanuit de originele zaak en verplaatst naar de Djuma zaak AVG?

Met opmerkingen [SP10R9]: Klopt, maar moet er niet met de G-schijf worden gewerkt om het antwoord te versturen?

Met opmerkingen [MD11]: Directeur Staf?

Met opmerkingen [SP12R11]: Ondertekening gebeurt door de FG.

- Of er sprake is van geautomatiseerde besluitvorming;
- Wanneer de persoonsgegevens niet bij de betrokkene zelf zijn verzameld, alle beschikbare informatie over de bron van de gegevens.

Overzicht NAW-gegevens in Djuma

Een opsomming in tabelvorm van de NAW-gegevens die van de betrokkene zijn vastgelegd in Djuma.

Overzicht dossiers

Een opsomming in tabelvorm van alle gevonden dossiers, het type dossier en een korte omschrijving van de dossiers.

3. Een versleutelde map met de persoonsgegevens

De verzamelde persoonsgegevens worden via een beveiligd uitwisselingsplatform (Secure Transfer) verstuurd. Hiervoor is een e-mailadres en telefoonnummer van indiener nodig. De indiener ontvangt via e-mail bericht dat er een gegevens klaar staan om te downloaden. Via een SMS bericht krijgt de indiener een code waarmee de gegevens kunnen worden gedownload.

Als er geen telefoonnummer van indiener bekend is, kan dit worden opgevraagd om de kopie van persoonsgegevens te kunnen versturen via een beveiligde manier. Indien indiener geen telefoonnummer wil verstrekken, wordt de informatie per e-mail verstuurd.

Als de indiener om een schriftelijke reactie per post vraagt worden de gevraagde persoonsgegevens geprint en samen met de begeleidende brief en bijlage aangetekend verstuurd.

In Djuma

De begeleidende brief, de bijlage en het e-mailbericht met de beantwoording wordt in Djuma vastgelegd als volgstuk in het AVG-dossier.

Met opmerkingen [MD13]: Het is uitgedraaid OF geprint.
Uitgeprint is dubbelop

4.8 Behandeling AVG-verzoek

Als de belangrijkste controles zijn uitgevoerd en de ontvangstbevestiging verzonden is, start de PO met de behandeling van het AVG-verzoek.

4.8.1 Verwijderverzoek

Beoordelen verwijderverzoek

De PO beoordeelt of (deels) gevolg moet worden gegeven aan het verzoek. Er kunnen wettelijke verplichtingen gelden waardoor we verplicht zijn persoonsgegevens voor een bepaalde periode te bewaren. De PO consulteert de archivaris hierover bij onduidelijkheid over de toepasselijke bewaartermijn(en).

De ombudsman is op grond van de Archiefwet verplicht om gegevens te bewaren volgens vastgestelde bewaartermijnen die zijn opgenomen in selectielijsten. Als de gegevens rechtmatig zijn verwerkt kunnen deze niet eerder worden verwijderd dan de vastgestelde bewaartermijn.

In deze situaties geldt het recht op verwijderen:

- De persoonsgegevens zijn niet meer nodig voor het doel waarvoor de gegevens zijn verzameld of waarvoor de gegevens worden verwerkt.
- De persoon in kwestie heeft eerder toestemming gegeven voor het gebruik van de gegevens, maar trekt die toestemming nu in.
- De persoon maakt (terecht) bezwaar tegen het gebruik van de gegevens.
- De organisatie houdt zich niet aan de privacyregels bij het gebruik van de persoonsgegevens. Bijvoorbeeld omdat er geen wettelijke grondslag is voor de verwerking.
- De organisatie is wettelijk verplicht om de gegevens na een bepaalde tijd te verwijderen.
- Apps en websites bij kinderen: de persoonsgegevens van een kind onder de 16 jaar zijn verzameld via een app of website.

In deze situaties geldt het recht op gegevens verwijderen niet:

- De verwerking van de gegevens is noodzakelijk om het recht op vrijheid van meningsuiting en informatie uit te oefenen. Daarmee doet de AVG recht aan het principe dat 'privacy' en 'vrijheid van meningsuiting' gelijkwaardige grondrechten zijn.
- De organisatie verwerkt de gegevens omdat er een wettelijke verplichting is om dat te doen.
- De organisatie verwerkt de gegevens om openbaar gezag of een (wettelijk vastgelegde) taak van algemeen belang uit te oefenen.
- De organisatie verwerkt de gegevens voor een taak van algemeen belang op het gebied van de volksgezondheid.
- De organisatie moet de gegevens in het algemeen belang archiveren.
- De gegevens zijn noodzakelijk voor een rechtsvordering.

[Inwilligen verwijderverzoek](#)

Het verzoek wordt ingewilligd, als er sprake is van een situatie waarbij het recht op verwijderen geldt.

De PO draagt zorg dat het verzoek wordt uitgevoerd en de betreffende gegevens worden vernietigd. De PO betreft zo nodig medewerkers die bevoegd zijn om de gegevens te vernietigen, bijvoorbeeld om het betreffende dossier te vernietigen.

Daarnaast verzoekt de PO aan betrokken medewerkers, zoals de behandelaar van een klachtdossier, om eventuele stukken met persoonsgegevens op andere plekken (G-schijf, outlook, etc.) te vernietigen.

[4.8.2 Verzoek tot rectificatie](#)

[Beoordelen verzoek tot rectificatie](#)

De PO beoordeelt of (deels) aan het verzoek tot rectificatie kan worden voldaan of niet.

Een betrokkene kan om rectificatie vragen in een van de volgende situaties:

- De persoonsgegevens kloppen niet;
- De persoonsgegevens zijn niet compleet.

Recht op rectificatie geldt niet als een betrokkene het niet eens is met een indruk, mening of conclusie van of inhoudelijke beoordeling door een medewerker. Feitelijke persoonsgegevens, zoals NAW-gegevens kunnen worden gerectificeerd. Mening en verslagleggingen niet.

Een verzoeker kan wel altijd vragen aan de behandelaar van het verzoekdossier om een toevoeging te doen aan het dossier.

[Inwilligen verzoek tot rectificatie](#)

Het verzoek wordt ingewilligd, als sprake is van een situatie waarbij het recht op rectificatie van toepassing is.

De PO draagt zorg dat het verzoek wordt uitgevoerd en kan hiervoor een actie uitzetten bij andere medewerkers, bijvoorbeeld medewerkers die bevoegd zijn om NAW-gegevens aan te passen in het systeem.

[4.8.3 Verzoek tot bezwaar](#)

[Beoordelen verzoek tot bezwaar](#)

De PO beoordeelt of (deels) aan het verzoek moet worden voldaan of niet. Het recht op bewaar kan alleen worden ingezet bij bijzondere persoonlijke omstandigheden.

Het recht op bezwaar geldt alleen als:

- De gegevens worden verwerkt voor een taak van algemeen belang of uitoefening van openbaar gezag;
- De gegevens worden verwerkt op basis van gerechtvaardigd belang; of
- De gegevens worden gebruikt voor profilering.

Als aan bovenstaande voorwaarden is voldaan dan moet de verwerking van de persoonsgegevens opnieuw worden bekeken en een afweging worden gemaakt. De PO doet dit in samenspraak met de FG. De gegevensverwerking moet worden gestopt tenzij er heel goede redenen zijn om de gegevens te blijven verwerken, die zwaarder wegen dan de belangen van de betrokkene.

[Inwilligen verzoek tot bezwaar](#)

Het verzoek wordt ingewilligd, als sprake is van een situatie waarbij het recht op bezwaar geldt en uit de afweging blijkt dat de gegevensverwerking moet worden gestopt.

De PO draagt zorg dat het verzoek wordt uitgevoerd en de betreffende gegevens worden vernietigd. De PO kan hiervoor een actie uitzetten bij andere medewerkers, bijvoorbeeld medewerkers die bevoegd zijn om dossiers te vernietigen in het zaakstelsel.

[4.8.4 Verzoek tot beperking](#)

[Beoordelen verzoek tot beperking](#)

De PO beoordeelt of (deels) aan het verzoek kan worden voldaan of niet. Beperking van de verwerking is mogelijk in de volgende situaties:

- De persoonsgegevens zijn mogelijk onjuist (en de betrokkene heeft een rectificatieverzoek ingediend);
- De verwerking van de gegevens is onrechtmatig (maar de betrokkene wil niet dat de gegevens worden verwijderd);
- De gegevens zijn niet meer nodig (maar de betrokkene wil niet dat de gegevens worden verwijderd, omdat die de gegevens nog nodig heeft voor een rechtsvordering);
- De betrokkene heeft bezwaar gemaakt tegen de verwerking van de gegevens vanwege de specifieke situatie van deze persoon (en het is nog niet duidelijk welk belang zwaarder weegt).

Indien niet aan een van bovenstaande voorwaarden is voldaan kan geen gevolg worden gegeven aan het verzoek.

[Inwilligen verzoek tot beperking](#)

Het verzoek wordt ingewilligd, als sprake is van een situatie waarbij het recht op beperking geldt.

De PO draagt zorg dat het verzoek wordt uitgevoerd en de betreffende gegevens niet worden gebruikt zolang het recht op beperking geldt. Het kan nodig zijn dat de toegang tot een dossier wordt beperkt om te voorkomen dat persoonsgegevens worden gebruikt.

[4.8.5 Verzoek tot overdraagbaarheid \(dataportabiliteit\)](#)

[Beoordelen verzoek tot overdraagbaarheid](#)

De PO beoordeelt of (deels) aan het verzoek kan worden voldaan of niet. Alleen gegevens die digitaal zijn vallen onder het recht op dataportabiliteit. Daarnaast geldt het recht alleen voor persoonsgegevens die worden verwerkt met iemands toestemming of als de gegevens nodig zijn om een overeenkomst met diegene uit te voeren.

Indien niet aan de voorwaarden is voldaan kan geen gevolg worden gegeven aan het verzoek.

[Inwilligen verzoek tot overdraagbaarheid](#)

Het verzoek wordt ingewilligd, als sprake is van een situatie waarbij het recht op overdraagbaarheid van toepassing is.

De PO draagt zorg dat het verzoek wordt uitgevoerd. Alle persoonsgegevens die de betrokkene aan ons heeft verstrekt, moeten beschikbaar worden gesteld. De gegevens moeten worden verstrekt in een gestructureerde, veelgebruikte en machineleesbaar formaat.

4.8.6 [Recht om niet onderworpen te zijn aan geautomatiseerde besluitvorming](#)

De ombudsman maakt bij de verwerking van persoonsgegevens geen gebruik van geautomatiseerde besluitvorming.

4.9 [AVG-Verzoek beantwoorden](#)

De PO informeert de indiener of wordt voldaan aan het verzoek. De beantwoording op een AVG-verzoek bestaat uit schriftelijk antwoord per e-mail of per brief.

Als niet kan worden voldaan aan het verzoek kan hiervoor tekst 3: 'AVG-recht niet van toepassing' uit Bijlage 1 worden gebruikt.

Als kan worden voldaan aan het verzoek kan hiervoor tekst 4 'AVG-recht van toepassing' uit Bijlage 1 worden gebruikt.

[Informeren andere organisaties](#)

De PO informeert andere organisaties aan wie de persoonsgegevens zijn versterkt, als gevolg wordt gegevens aan het recht op rectificatie, verwijdering, beperking van de verwerking of bezwaar.

In Djuma

Het e-mailbericht met de beantwoording en eventueel de begeleidende brief wordt in Djuma vastgelegd als volgstuk in het AVG-dossier.

Bijlage A Begrippenlijst

Begrip	Toelichting
PO	De Privacy Officer is verantwoordelijk voor de operationele uitvoering van taken die voortvloeien uit de AVG.
AVG-vertegenwoordiger	Een medewerker van een team of domein die als aanspreekpunt fungeert voor AVG vragen.
Indiener	Dit is degene die feitelijk het inzageverzoek indient. In de meeste gevallen is de indiener ook de betrokkene. De indiener kan een burger maar ook een wettelijk vertegenwoordiger, bewindvoerder, gemachtigde of intermediair zijn.
Betrokkene	Dit is een natuurlijk persoon die op basis van persoonsgegevens direct of indirect kan worden geïdentificeerd.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (tekst afkomstig uit AVG).
Veelvrager	Dit is een indiener of betrokkene die buitensporig veel inzageverzoeken indient.
Derde	Dit is een natuurlijk persoon van wie zijn persoonsgegevens bij het verzamelen van een inzageverzoek naast die van de betrokkene ook inzichtelijk zijn geworden, maar waarvan deze gegevens niet er inzage gegeven/verstrekt worden aan de betrokkene.

Bijlage B Modelteksten

Ontvangstbevestiging

Tekst 1: Standaard ontvangstbevestiging.

Geachte **<naam betrokkene>**,

De Ombudsman heeft op **<datum>** uw verzoek op basis van de AVG van **<datum>** ontvangen. Uw verzoek wordt in behandeling genomen en u verneemt zo snel mogelijk, uiterlijk binnen vier weken, nader bericht.

Indien uw verzoek complex van aard of veel omvattend blijkt te zijn is het mogelijk dat de reactietermijn verlengd wordt met maximaal twee maanden. U wordt daarvan binnen één maand op de hoogte gebracht.

Met vriendelijke groet,

<ondertekening PO>

Tekst 2: Aanvulling op ontvangstbevestiging indien identificatie nog niet is vastgesteld.

Om uw identiteit deugdelijk vast te kunnen stellen hebben we aanvullende informatie nodig. Ter bevestiging van uw identiteit verzoek ik u mij zo spoedig mogelijk een kopie van een geldig identiteitsbewijs te sturen.

Hoe u een veilige kopie maakt vindt u hier:

<https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/veilige-kopie-identiteitsbewijs?>

De kopie van uw identiteitsbewijs wordt direct vernietigd zodra uw identiteit is vastgesteld.

Besluit geen gevolg/beperking AVG-verzoek

Tekst 1: Geen gevolg geven aan het verzoek

Geachte <naam betrokkene>,

Naar aanleiding van uw AVG-verzoek van <datum verzoek> bericht ik u als volgt.
Er wordt geen gevolg gegeven aan uw verzoek, omdat <reden afwijzing>.

Als u niet tevreden bent met de wijze waarop uw verzoek is afgehandeld, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

Tekst 2: Beperking van het verzoek

Geachte <naam betrokkene>,

Naar aanleiding van uw AVG-verzoek van <datum verzoek> bericht ik u als volgt. Er is een wettelijke grondslag die maakt dat uw verzoek wordt beperkt. Beperking van uw verzoek is een noodzakelijke en evenredige maatregel ter waarborging van <reden genoemd in art. 23 sub a t/m j AVG>.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

Antwoorden op het AVG-verzoek

Tekst 1: Geen persoonsgegevens aanwezig

Geachte **<naam betrokkene>**,

Naar aanleiding van uw verzoek van **<datum verzoek>** bericht ik u als volgt. U bent bij de Nationale ombudsman niet bekend. Er worden geen persoonsgegevens van u door de Nationale ombudsman verwerkt.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

Tekst 2: Verstrekken kopie persoonsgegevens

Geachte **<naam betrokkene>**,

In de bijgevoegde brief treft u het antwoord van de Nationale ombudsman aan op uw AVG-verzoek om inzage in uw persoonsgegevens.

U ontvangt apart een e-mailbericht met een Secure Transfer link naar [een Excel bestand met daarin een overzicht van de gevraagde persoonsgegevens/de afschriften van de stukken waarin uw persoonsgegevens zijn opgenomen].

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

Tekst 3: AVG-recht niet van toepassing

Geachte **<naam betrokkene>**,

Naar aanleiding van uw verzoek van **<datum verzoek>** bericht ik u als volgt.

U verzoekt om **<AVG-recht>** met betrekking tot dossier met zaaknummer **<nummer>**. Het recht op **<AVG-recht>** geldt alleen in bepaalde situaties. Zie voor meer informatie de website van de Autoriteit Persoonsgegevens **<link>**.

Het recht op **<AVG-recht>** is hier niet van toepassing.

Als u niet tevreden bent met de wijze waarop uw verzoek is afgehandeld, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

Tekst 4: AVG-recht van toepassing

Geachte **<naam betrokkene>**,

Naar aanleiding van uw verzoek van **<datum verzoek>** bericht ik u als volgt.

U verzoekt om **<AVG-recht>** met betrekking tot dossier met zaaknummer **<nummer>**. Het recht op **<AVG-recht>** is hier van toepassing.

Als u niet tevreden bent met de wijze waarop uw verzoek is afgehandeld, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens. Meer informatie vindt u op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

<ondertekening PO>

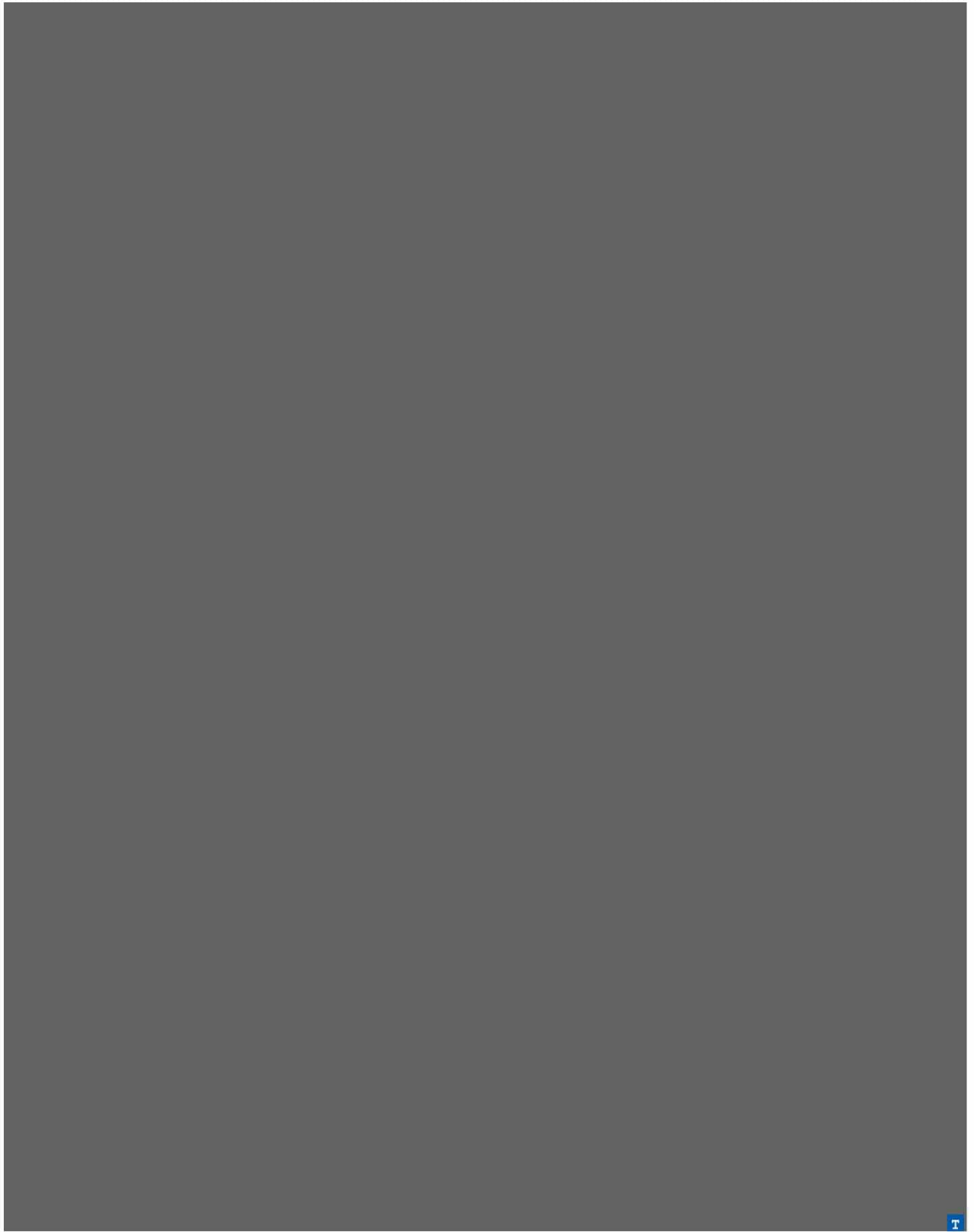
Personeelshandboek 2022

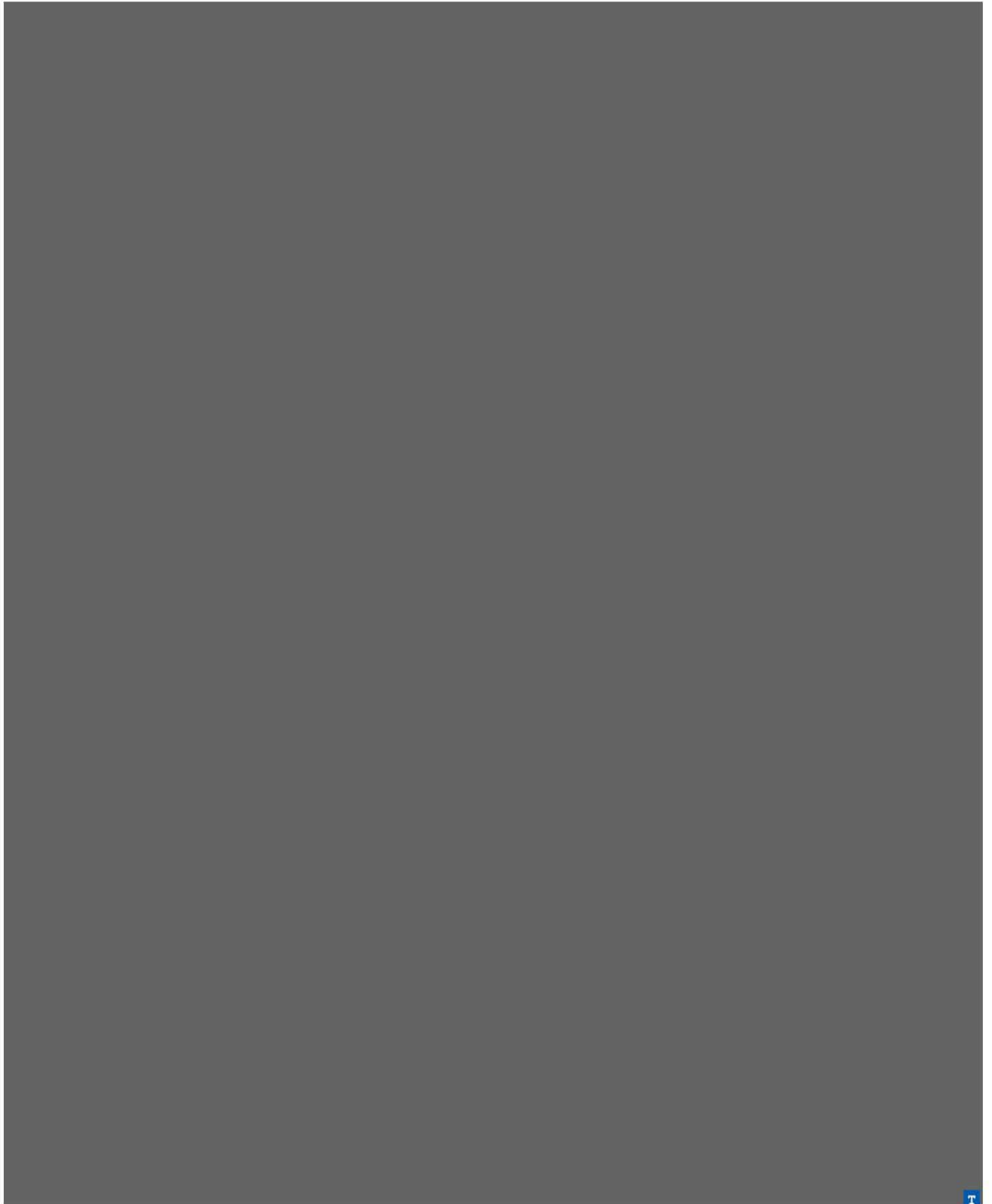


Inhoudsopgave

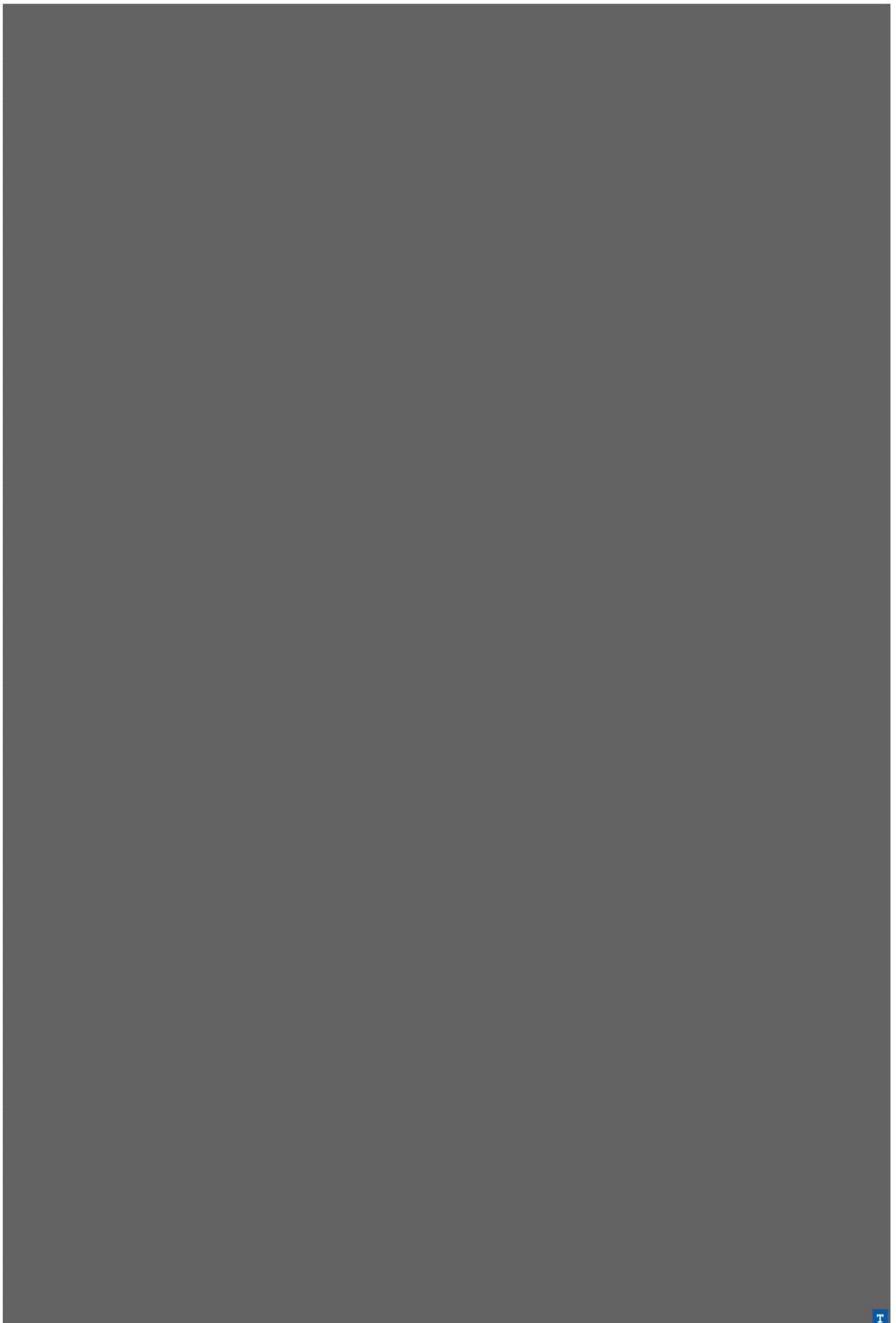
Gedragsregels gebruik zakelijke laptop	10
Gedragsregeling mobiele telefonie	11
Hoofdstuk 3: Veilig omgaan met informatie	
Beveiligingsbeleid	15
Beleid bescherming persoonsgegevens en AVG	16

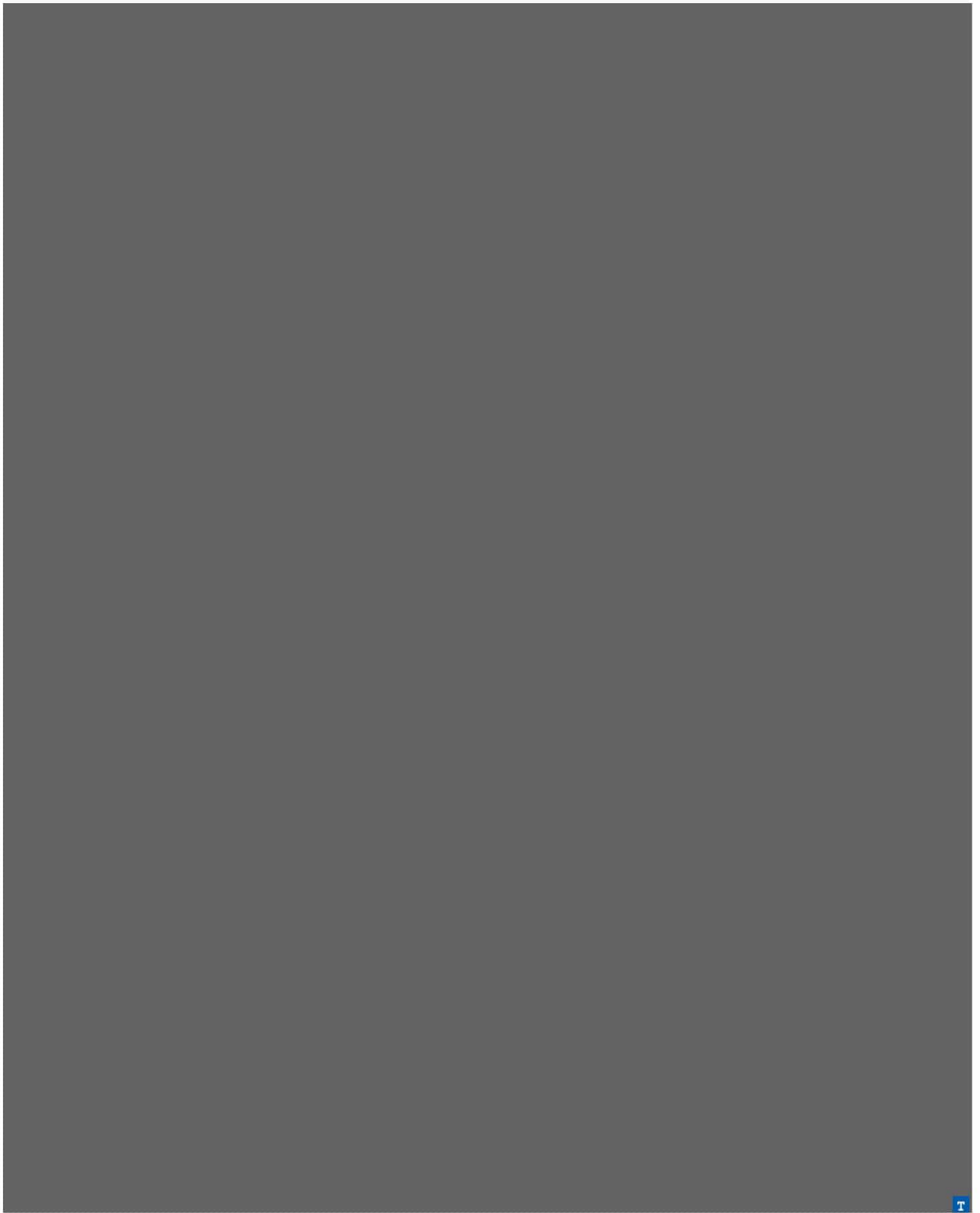


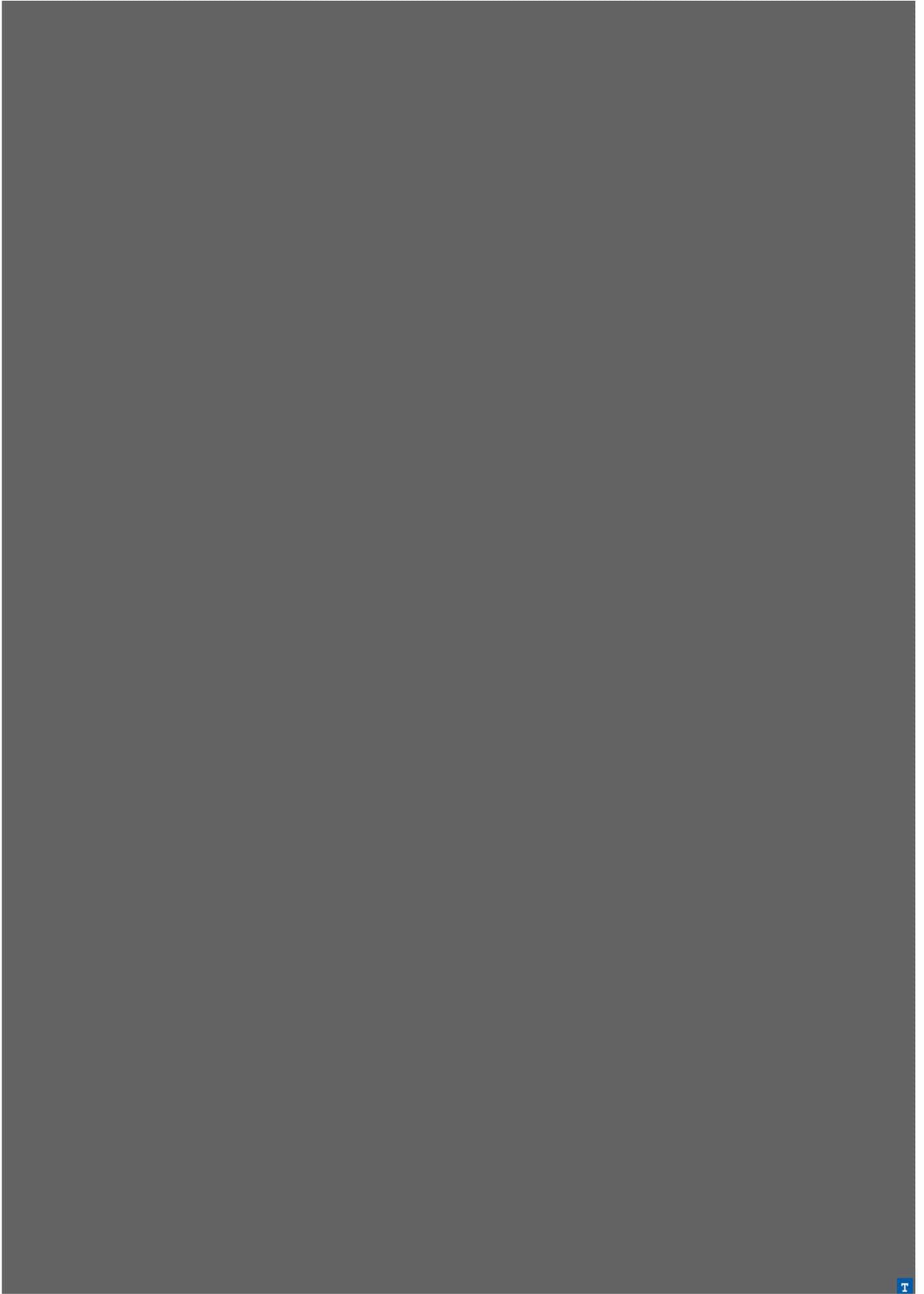












T



Gedragsregels gebruik zakelijke laptop

Als medewerker krijg je de beschikking over een laptop en accessoires. Het is van belang dat je je bewust bent van de rechten en plichten en risico's die het gebruik van deze laptop met zich meebrengen. Deze gedragsregels beschrijven het van jouw gewenste gedrag bij gebruik van de zakelijke laptop en toebehoren en geeft een algemene toelichting.

Gebruik van de laptop

De laptop is persoonlijk en uitsluitend bedoeld voor zakelijk gebruik. Het is niet toegestaan de laptop uit te lenen aan derden.

Het is niet toegestaan om (privé) software te installeren op de laptop. Als je software nodig hebt wat niet beschikbaar is, geef dit dan aan bij je leidinggevende zodat bekeken kan worden of de gevraagde software beschikbaar kan worden gesteld.

De laptop geeft een grote mate van mobiliteit. Wanneer je buiten kantoor op een publieke locatie aan het werk bent, houd dan rekening met meelezers en bekijk geen gevoelige stukken op je laptop.

Als je van je werkplek afloopt, vergrendel dan je laptop. Laat je laptop niet onbeschermd achter als je voor langere tijd van je plek af bent.

Als je je laptop bent vergeten mee te nemen en je wilt op kantoor werken, dan heb je geen werkplek. De afdeling ICT geeft in dat geval geen tijdelijke laptop.

Transport

De laptop wordt geleverd met een tas. Er wordt van je verwacht dat je bij transport buiten kantoor of woning de laptop goed beschermd. Het is toegestaan om een eigen tas te gebruiken waar de laptop in past. Aanschaf van een eigen tas is voor eigen rekening. Als je twijfelt of je eigen tas voldoende bescherming biedt, dan kun je dit voorleggen aan een medewerker van ICT.

Verlies of diefstal

Bij verlies of diefstal moet je aangifte te doen bij de politie. Ook moet je melding doen bij je leidinggevende en de afdeling ICT. Het melden van diefstal of verlies moet direct gebeuren, ongeacht dag of tijdstip. Dit kan telefonisch via  of per e-mail via @nationaleombudsman.nl). Het is van belang dat ICT de toegang tot de laptop en digitale omgeving van de Nationale ombudsman zo snel mogelijk kan blokkeren.

Een kopie van aangifte bij de politie moet ingeleverd worden bij ICT voor registratie in Topdesk. Na melding kan je een nieuwe laptop afhalen bij ICT.

Schade

Bij dagelijks gebruik van de laptop kan er schade ontstaan aan het apparaat. We onderscheiden twee soorten schades:

1. Lichte schade (gebruikssporen);
Denk hierbij aan krasjes in de behuizing. Deze schade valt in de categorie gebruikssporen en hoeft niet gemeld te worden.
2. Schade waardoor werken bemoeilijkt wordt.
Denk hierbij aan toetsen die niet meer werken, een barst in het scherm, schade waardoor werken op de laptop beperkt of zelfs onmogelijk is. Meldt de schade bij de afdeling ICT. ICT bekijkt dan of de schade direct te herstellen is. Als dit niet het geval is, dan wordt een nieuw apparaat in gebruik gegeven.

Gedragsregeling mobiele telefonie

Als medewerker krijg je de beschikking over een mobiele telefoon, oplader en headset. Respecteer het feit dat het om overheidsmiddelen gaat en die zijn gegeven om te gebruiken voor het werk. Gebruik ze voor het doel waarvoor je ze hebt gekregen en ga er voorzichtig en zuinig mee om.

Gepast privégebruik toegestaan

Bij moderne arbeidsverhoudingen past het niet om privégebruik geheel te verbieden. Omgekeerd zul je ook wel eens eigen middelen gebruiken voor het werk. Gepast gebruik mag. Misbruik, dat wil zeggen overmatig, uitbundig, onnodig, storend of schadelijk privégebruik is niet toegestaan.

Het is ondoenlijk om vooraf precies aan te geven wanneer er sprake is van misbruik en wanneer niet. We doen daarom een beroep op je eigen verantwoordelijkheid en oordeelsvermogen. Houd daarbij voor ogen dat het rijksmiddelen zijn die uit belastinggeld worden gefinancierd. Er is altijd sprake van grijs gebied: bespreek daarom in voorkomende gevallen met je leidinggevende wat wel en wat niet mag. Wees transparant en maak hierover afspraken.

De afdeling ICT

- Heb je hulp nodig, omdat je bijvoorbeeld niet weet of bepaalde software (app) die je wilt installeren wel veilig is, dan helpt ICT je graag.
- ICT monitort het verbruik aan de hand van de factuurbedragen van de provider. Kosten die voortvloeien uit bovenmatig privégebruik kunnen worden verhaald.
- Zakelijke aankopen schiet je zelf voor.

Wat te doen bij verlies of diefstal?

- Meldt diefstal of het verlies direct bij ICT, ongeacht de dag of het tijdstip. Betreft het je mobieltje dan kunnen de gegevens zo snel mogelijk worden verwijderd. ICT is telefonisch bereikbaar via [REDACTED] of per e-mail via [REDACTED]@nationaleombudsman.nl.
- Doe hiervan aangifte bij de politie.
- Meldt diefstal of verlies bij je leidinggevende.
- Een kopie van de aangifte bij de politie lever je per mail in bij Chief Information Security Officer.
- ICT zorgt voor vervanging van het bedrijfsmiddel.

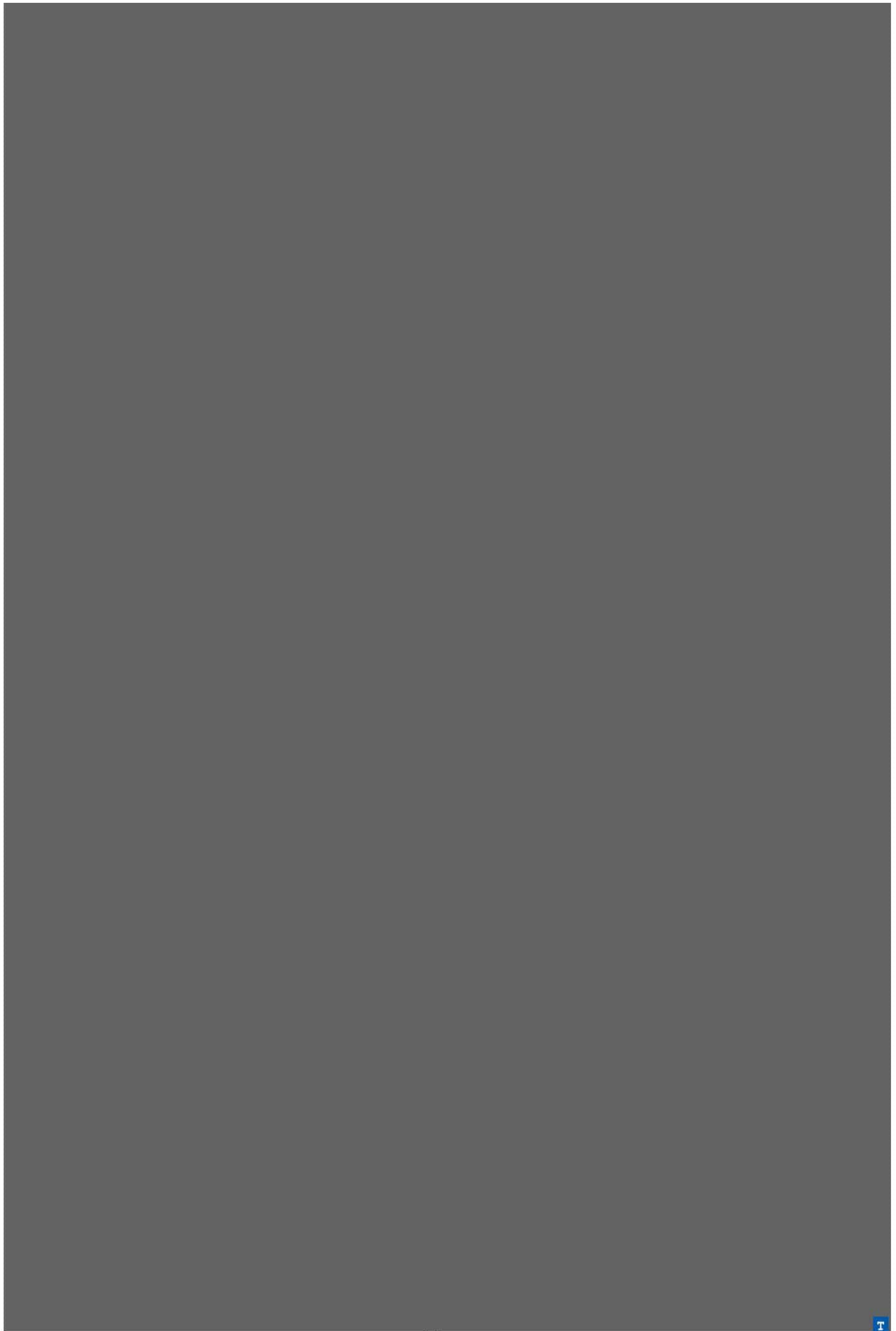
Wat te doen bij schade en defecten?

Bij dagelijks gebruik is het niet ondenkbaar dat er schade aan het apparaat ontstaat.

We maken onderscheid in twee soorten schades:

1. Gebruikerssporen;
Denk hierbij aan krasjes in de behuizing. Deze schade valt in de categorie gebruikssporen en hoeft niet gemeld te worden.
2. Schade waardoor werken bemoeilijkt wordt.
Denk bijvoorbeeld aan een kras of barst in het scherm, de batterij snel leegloopt of wanneer de oplader kapot is.

Meld de schade bij de afdeling ICT. ICT bekijkt dan of dit direct te herstellen is. Als dit niet het geval is, dan wordt er voor (tijdelijke) vervanging gezorgd. ICT bepaalt waar en door wie de schade of het defect wordt hersteld.







Hoofdstuk 3: Veilig omgaan met informatie

Beveiligingsbeleid

Beveiliging van informatie en personen

Het doel van dit beleid is om de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau, te beperken. Dit is vastgelegd in het Informatiebeveiligingsbeleid. Naast een veilige ICT-omgeving of een veilige kantoor-omgeving gaat het hierbij ook over genomen maatregelen om verstandig om te kunnen gaan met informatie, eerlijk en integer handelen en veiligheid op het werk.

Zorgvuldig omgaan met informatie

Voor medewerkers en stagiaires is daarom een leeswijzer ontwikkeld die een overzicht geeft van alle regels en afspraken over dit onderwerp. In de leeswijzer staan onder andere de afspraken over het ontvangen van bezoekers, het omgaan met vertrouwelijke informatie en wat te doen bij een datalek. Maar ook staat beschreven wat we verstaan onder eerlijk en integer handelen. De leeswijzer vind je hier.

Bij wie moet je zijn?

De coördinatie van het beveiligingsbeleid ligt bij Chief Information Security Officer (CISO),  t, die tevens informatiemanager is. Hij is verantwoordelijk voor het maken van beleid en moet ervoor zorgen dat medewerkers goed zijn geïnformeerd. Bij de informatiemanager kun je terecht voor opmerkingen en/of vragen over dit onderwerp.

Wil je weten waar de verantwoordelijkheden van de verschillende de onderdelen van informatiebeveiliging liggen, kijk dan in de leeswijzer.

Beveiligingsincident

Of het nu gaat om een phishingmail, een vermoedelijk datalek, diefstal of een indringer in het pand, alle beveiligingsincidenten willen we zo snel en goed mogelijk behandelen. Daarom is snelle melding een belangrijk startpunt. Dus heb je het vermoeden van een beveiligingsincident, bel dan meteen de ICT-helpdesk. Dit kan bijvoorbeeld als je per ongeluk op een kwaadaardig linkje hebt geklikt. (Er hoeft dan niet altijd direct iets vreemds te gebeuren. Het devies is daarom: bij twijfel, bellen.)

Een datalek meld je onmiddellijk en uiterlijk binnen 24 uur via het meldingsformulier. Ook meld je het incident aan je leidinggevende. Het meldingsformulier vind je hier.

Tips en trucs voor het veilig omgaan met informatie

Er zijn negen gouden tips ontwikkeld om goed om te gaan met informatiebeveiliging. Deze tips vind je hier.

Interventieteam

Bij het ontstaan van een gevaarlijke situatie kun je via de receptie het interventieteam oproepen voor ondersteuning.

Beleid bescherming persoonsgegevens en AVG

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dat betekent dat dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De AVG biedt het waarborgen voor de bescherming van de persoonlijke levenssfeer van natuurlijke personen met betrekking tot het verwerken van persoonsgegevens.

De Nationale ombudsman verwerkt in het kader van het primair proces en haar bedrijfsvoering persoonsgegevens en vindt het belangrijk dat er met deze persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk moeten worden behandeld.

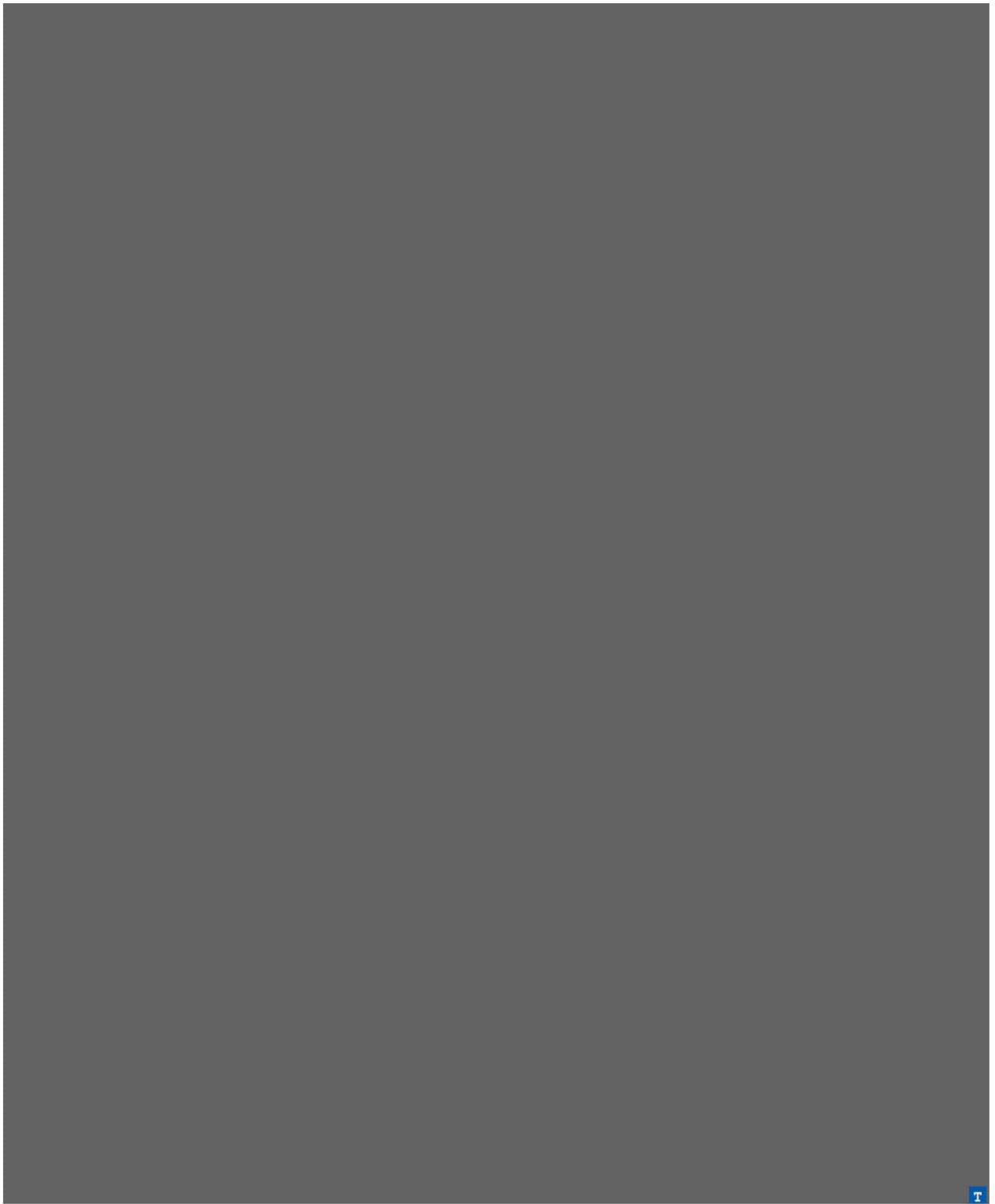
De Nationale ombudsman heeft, in lijn met wat in de AVG-wetgeving staat, een beleid opgesteld voor het gebruik van persoonsgegevens. Het beleid vind je [hier](#). In het bestand wordt uiteengezet wat het Beleid Bescherming Persoonsgegevens inhoudt en hoe dit door alle medewerkers van de Nationale ombudsman zal moeten worden nageleefd. Dit zodat betrokkenen ervan op aan kunnen dat met persoonsgegevens veilig en verantwoord wordt omgegaan door de medewerkers van de Nationale ombudsman.

Het beleid heeft als doel:

- Regels te stellen voor het verwerken van persoonsgegevens door de medewerkers van de Nationale ombudsman;
- Informatie te verschaffen aan personen van wie persoonsgegevens door de medewerkers van de Nationale ombudsman verwerkt (zullen) worden;
- Bij te dragen aan de transparantie van de regels die door de Nationale ombudsman worden toegepast bij het verwerken van persoonsgegevens.

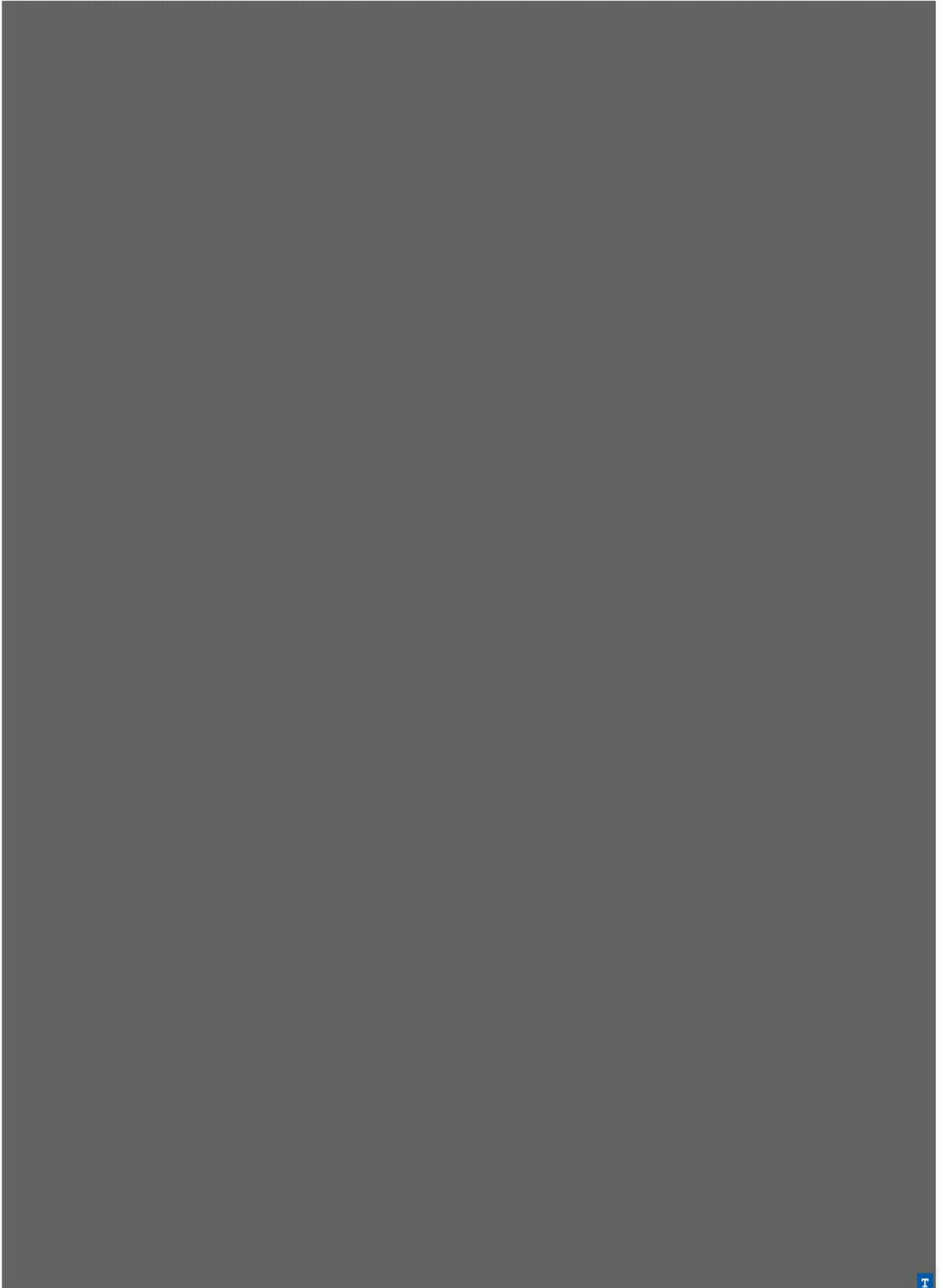
Vragen?

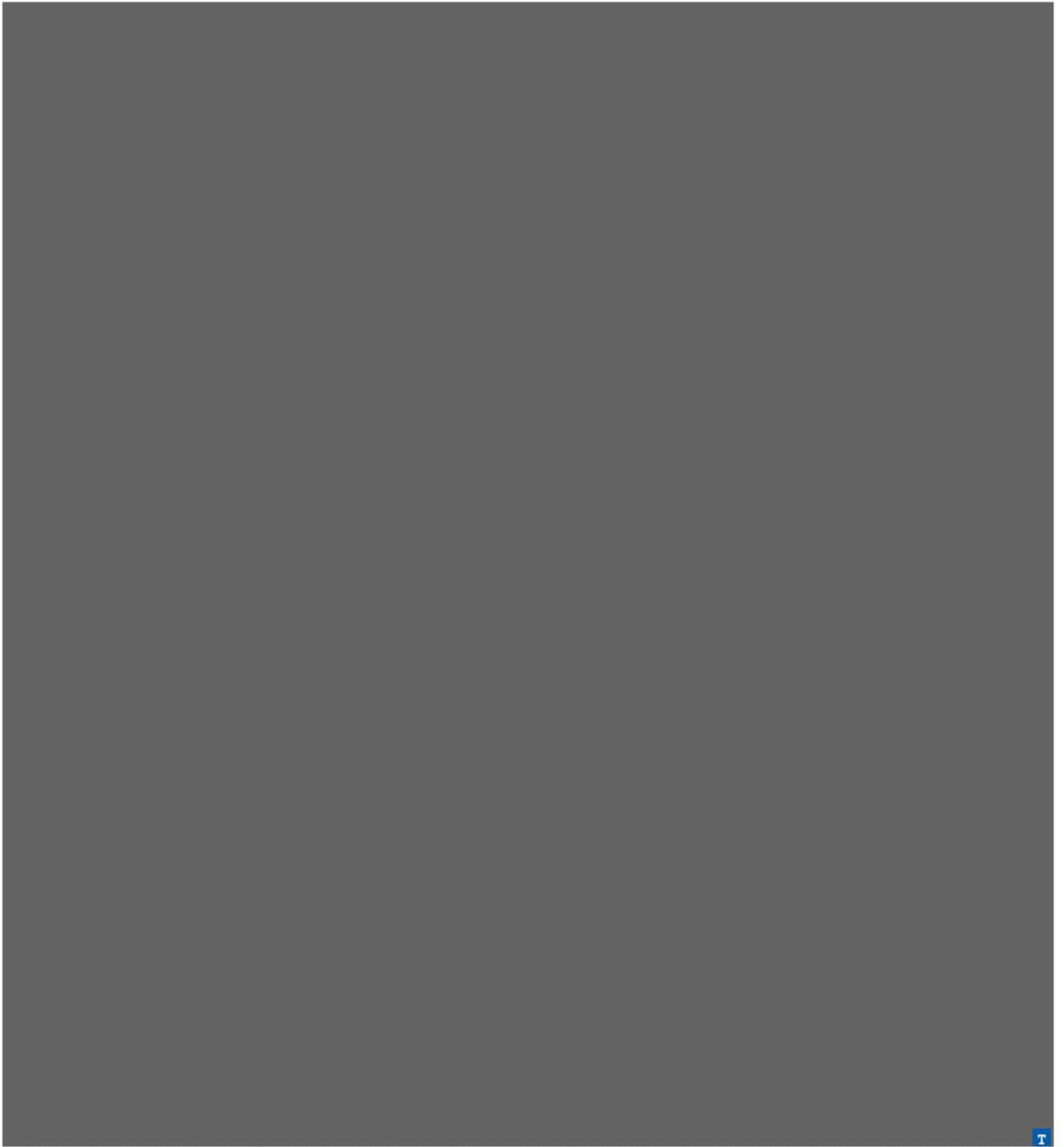
Heb je een concrete vraag over de toepassing van de privacyregelgeving in je dagelijkse werk, dan kun je die stellen aan de AVG-vertegenwoordiger van je sector of afdeling. Overige vragen kun je sturen naar het e-mailadres: @nationaleombudsman.nl.

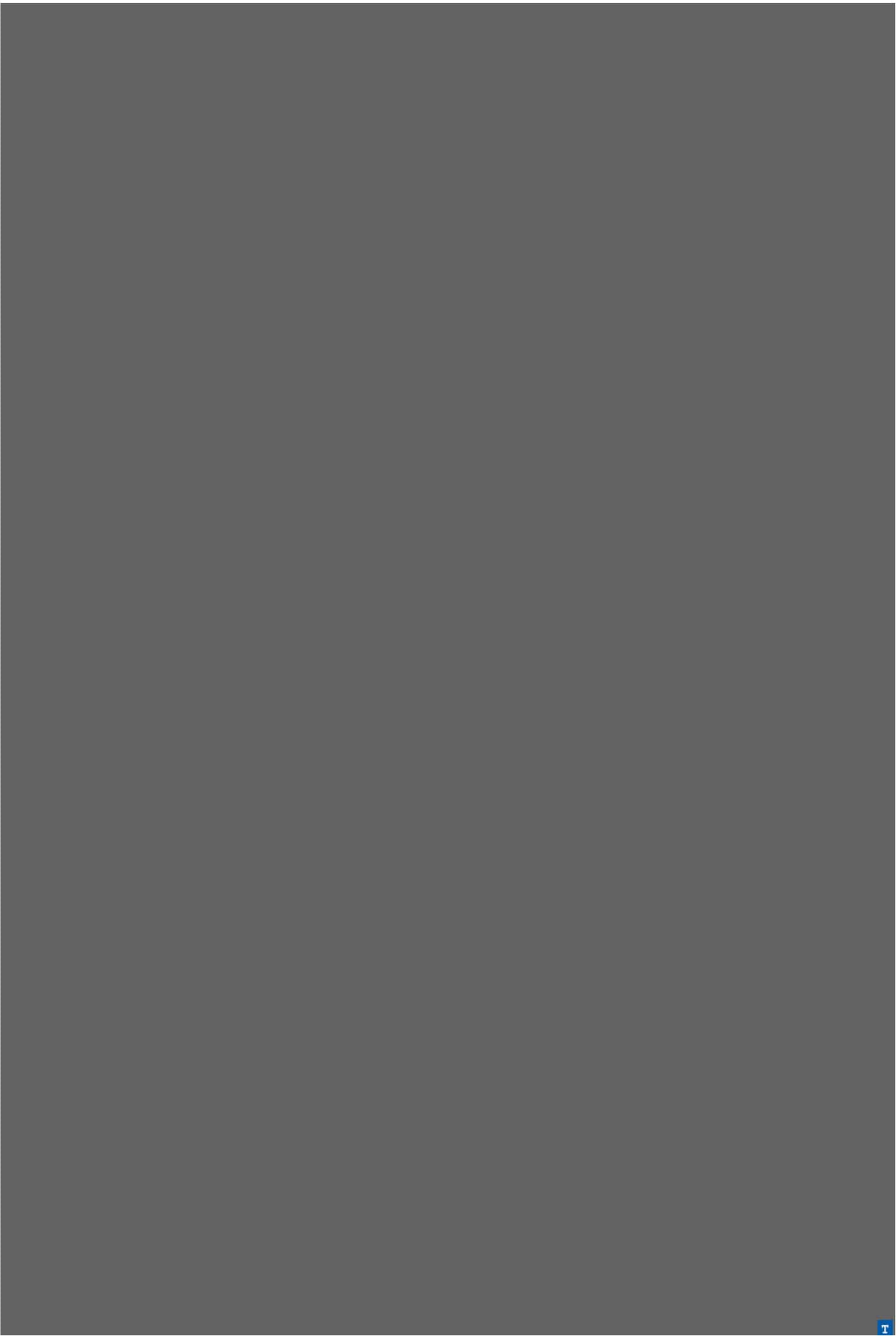




T



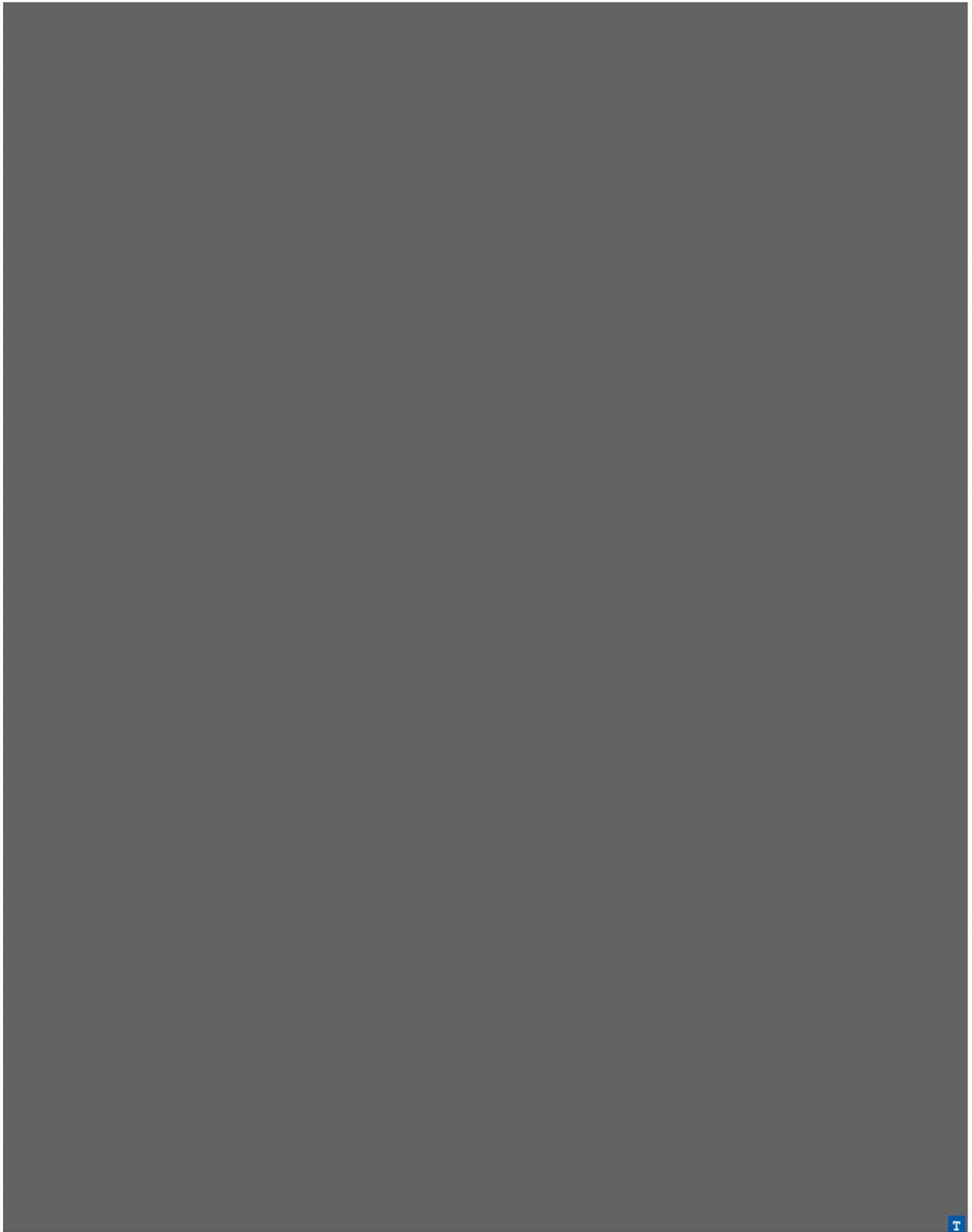


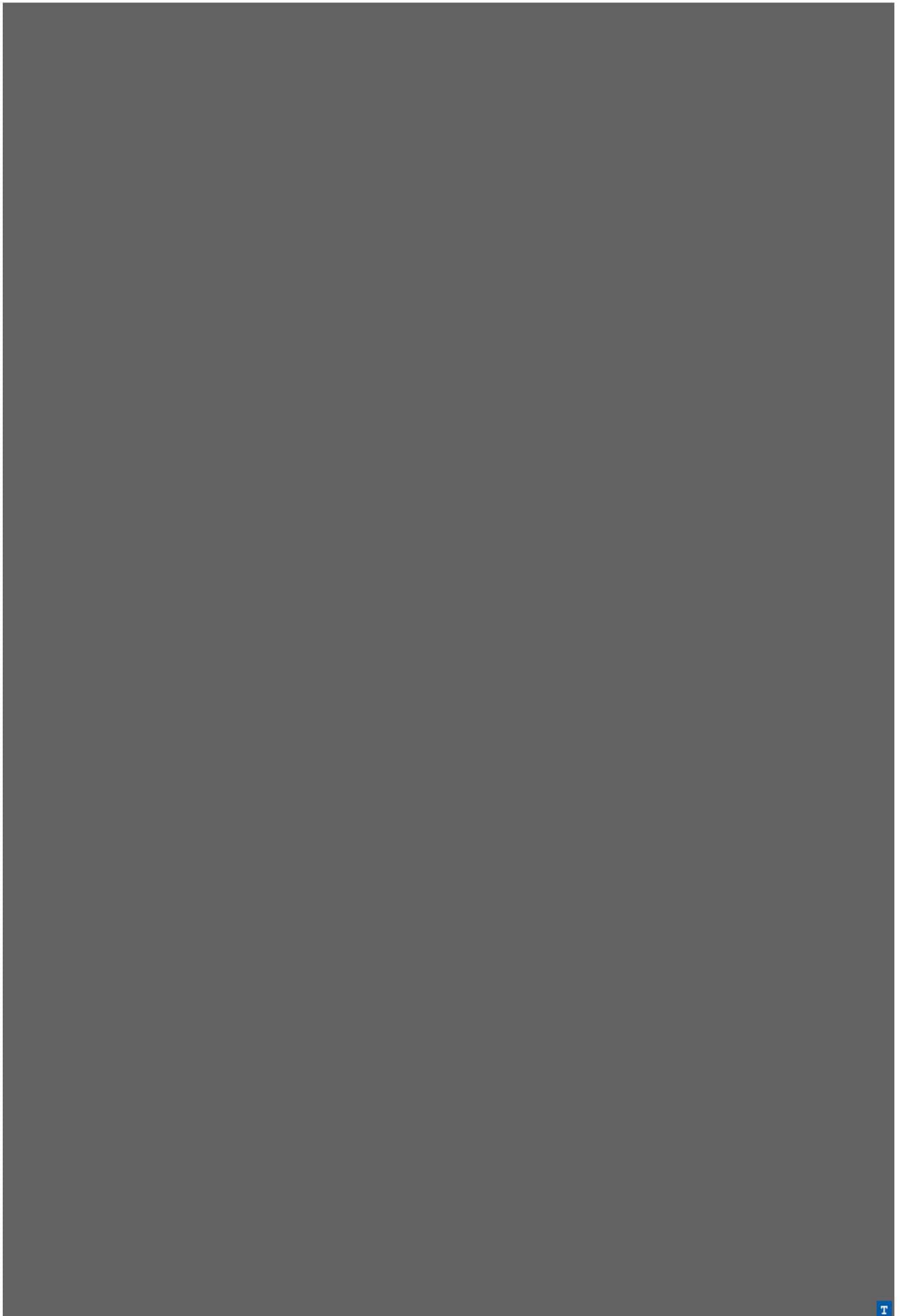


T















T

