nationale ombudsman

Retouradres: Postbus 93122, 2509 AC Den Haag

[redacted]

Geachte [redacted]

Datum
3 mei 2024

Onderwerp
Woo-besluit datalekken 2020-2021

Ons nummer
1951369

Uw kenmerk

Bijlage(n)
5

Contactpersoon
[redacted]
T 070 [redacted]

Op 29 maart 2024 heeft de Nationale ombudsman uw verzoek om informatie over datalekken ontvangen. U doet hierbij een beroep op de Wet open overheid (Woo).

Uw verzoek
U vraagt om de volgende informatie:
1. Alle in documenten vastgelegde communicatie over concrete gevallen van (vermeende) datalekken die zich in de periode 1 januari 2020 tot en met 31 december 2021 bij de Nationale ombudsman hebben voorgedaan. Bijvoorbeeld: een e-mail van een medewerker waarin melding wordt gemaakt van een (vermeend) datalek, notulen van overleggen waarin (vermeende) datalekken worden besproken, meldingen aan de Autoriteit Persoonsgegevens, terugkoppeling van de Autoriteit Persoonsgegevens, melding naar persoon waarop het datalek ziet, een extern advies over een concreet (vermeend) datalek, het datalekregister etc.
2. Documenten ten aanzien van procedures en beleid ten aanzien van datalekken.
3. Audits ter voorkoming van datalekken.

Reden van uw verzoek is dat u ziet dat overheidsorganisaties verschillend met datalekken omgaan. U verwacht dat met de openbaar te maken documenten inzicht wordt gegeven in hoe de Nationale ombudsman omgaat met datalekken.

Besluit
Op basis van uw verzoek is gezocht naar de informatie in ons zaaksysteem en op de netwerkschijven. Er zijn vier documenten gevonden en er is één document gegenereerd. Deze vijf documenten geven inzicht in hoe de Nationale ombudsman omgaat met datalekken.
De volgende documenten horen bij dit besluit:

1. Overzicht van (vermeende) datalekken over de periode van 1 januari 2020 tot en met 31 december 2021.
2. Tekststandaarden berichtgeving datalekken.
3. Reactie (ontvangstbevestiging) van Autoriteit Persoonsgegevens.
4. Protocol datalekken.
5. Formulier melden datalek.

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

Toelichting op het besluit
Hieronder ga ik, per onderdeel, in op uw verzoek.
Verzoek 1
U vraagt om alle in documenten vastgelegde communicatie over concrete gevallen van (vermeende) datalekken. U geeft daarbij voorbeelden aan. Zo vraagt u om meldingen naar de persoon waarop het datalek ziet. Uitgangspunt van de Woo is dat informatie in de vorm van bestaande documenten openbaar worden gemaakt. De Woo verplicht niet om documenten te generen. In dit geval wijk ik af van dit uitgangspunt en heb ik een overzicht gemaakt van de meldingen. Hier is voor gekozen omdat de informatie op deze manier overzichtelijker openbaar kan worden gemaakt. Daarbij is het niet nodig om de afzonderlijke documenten te anonimiseren. Het overzicht is gegenereerd uit het datalekregister. Dit betreft het document met nummer 1.
In document 2 zijn zeven tekststandaarden opgenomen die gebruikt worden bij de berichtgeving over datalekken naar de betrokken personen.
1 en 2 gecombineerd geven het antwoord op dit punt van uw verzoek.
Ik besluit deze twee documenten in zijn geheel openbaar te maken.

In ons systeem is één document gevonden dat ziet op de terugkoppeling van de Autoriteit Persoonsgegevens. Dit met 3 genummerd document betreft een ontvangstbevestiging van het gemelde datalek.
Op grond van artikel 5.1, tweede lid, aanhef en onder e, van de Woo kan ik geen informatie aan u verstrekken als dit de persoonlijke levenssfeer schaadt en dit belang zwaarder weegt dan het algemeen belang om toegang te hebben tot de informatie. Het gaat in dit geval om persoonsgegevens in de vorm van namen, telefoonnummers en mailadres die (indirect) te herleiden zijn tot deze medewerkers. Ik vind het in dit geval belangrijk dat de identiteit van betrokkenen niet bekend wordt omdat dit hun privacy kan schenden.
Ik besluit voor dit document uw verzoek deels in te willigen en deels af te wijzen.

Er zijn geen documenten gevonden over de door u aangegeven voorbeelden in de vorm van notulen, extern advies en meldingen aan de Autoriteit Persoonsgegevens. Meldingen vinden plaats op de site van de Autoriteit Persoonsgegevens en deze berusten dan ook niet bij de Nationale ombudsman.

Verzoek 2
De documenten 4 en 5 zien op de procedures en beleid ten aanzien van datalekken. In deze documenten is informatie onleesbaar gemaakt.
Op grond van artikel 5.1, tweede lid, aanhef en onder e, van de Woo kan ik geen informatie aan u verstrekken als dit de persoonlijke levenssfeer schaadt en dit belang zwaarder weegt dan het algemeen belang om toegang te hebben tot de informatie. Het gaat in dit geval om een persoonsgegeven in de vorm van een mailadres dat (indirect) te herleiden is tot een medewerker. Ik vind het in dit geval belangrijk dat de identiteit van betrokkene niet bekend wordt omdat dit zijn privacy kan schenden.
Ik besluit voor deze documenten uw verzoek deels in te willigen en deels af te wijzen.

Verzoek 3
Er zijn geen documenten aangetroffen die zien op audits ter voorkoming van datalekken. Op dit punt kan ik uw verzoek niet inwilligen.

Wijze van bekendmaking
Naast dat het besluit met bijlagen aan u wordt toegezonden, zal het (geanonimiseerde) verzoek, het (geanonimiseerde) besluit en het overzicht worden gepubliceerd op onze website.

Nog 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 (1951369) te vermelden.

Met vriendelijke groet,
de Nationale ombudsman,
namens deze,

[redacted]

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.

Overzicht datalekken 1 januari 2020 – 31 december 2021

	Datum melding	Gemeld aan AP	Omschrijving	Aard datalek	Maatregelen
1	2-12-2021	Niet gemeld aan AP	Datalek: UWV formulier aangetroffen in laptoptas	Bij uitgifte laptop aan nieuwe collega is een UWV formulier aangetroffen met gegevens van een burger of (ex)collega.	Vastgesteld van wie de brief is. Brief is aangetekend verzonden naar de eigenaar.
2	25-11-2021	Niet gemeld aan AP	Datalek, mail per ongeluk naar interne mailgroep	de e-mail bevat: - aantal namen van klachtencommissie - naam, e-mailadres verzoeker	- emailgroep is verwijderd - ontvangers zijn op de hoogte gesteld dat bericht niet voor hen bedoeld is.
3	17-11-2021	Niet gemeld aan AP	Vermoedelijk datalek: poststuk naar oud adres verstuurd	Kopie dossier dat vz bij ons opvroeg is naar zijn vorige woonadres verstuurd.	- bij verzoeker navragen wat contactgegevens van verhuurder zijn en verhuurder vragen poststuk te retourneren. - Verzoeker gaat zelf poststuk ophalen op adres. Zonder tegenbericht is dit gelukt. Geen tegenbericht ontvangen.
4	12-11-2021	Niet gemeld aan AP	Datalek: e-mail naar verkeerde ontvanger	Dit e-mailbericht bevat het e-mailadres van verzoeker.	- de onterechte ontvanger wordt op de hoogte gesteld en verzocht het bericht te verwijderen. - de verzoeker wiens e-mail is mee verzonden wordt op de hoogte gesteld.
5	5-11-2021	Niet gemeld aan AP	Datalek: e-mails naar verkeerde geadresseerde	Naast persoonsgegevens van verzoeker worden ook 2 namen van politieambtenaren genoemd.	De e-mails zijn wel afgeleverd op het e-maildomein politie.nl alleen bij navraag niet bij een bestaand persoon. Geen verdere actie nodig.
6	25-10-2021	Niet gemeld aan AP	Datalek mail naar verkeerde gemeente	Klacht van verzoeker is doorgestuurd naar contactpersoon gemeente Oisterwijk en was bestemd voor gemeente Oirschot. Gemeente Oirschot heeft contact opgenomen om te melden dat bericht niet voor hen bestemd was.	Geen verdere actie nodig omdat gemeente mail heeft verwijderd.
7	6-10-2021	Niet gemeld aan AP	Datalek: e-mailbericht naar verkeerde ontvanger	Het e-mailbericht bevat een klachtomschrijving van de indiener, de naam van een klachtbehandelaar en emailadressen van 2 medewerkers en van de indiener zelf.	In forcepoint check uitgevoerd. Mail naar verkeerd adres is afgeleverd. vervolgstappen: - mail met verzoek verwijderen e-mails naar verkeerde adres.

8	14-9-2021	Niet gemeld aan AP	Datalek; e-mail naar verkeerd geadresseerde	E-mailbericht gestuurd naar een aantal ontvangers waaronder een externe verkeerd geadresseerde. Verkeerd geadresseerde heeft direct gereageerd. E-mail bevatte geen gevoelige gegevens. Betrokken persoonsgegevens: - e-mailadressen en namen van 6 collega's.	Geen verdere actie nodig omdat mail is verwijderd door melder.
9	2-9-2021	Niet gemeld aan AP	Datalek: interne mail naar extern contactpersoon	E-mailbericht bevat: namen van 3 onderzoekers, achternaam verzoeker. Verder geen informatie wat een risico zou kunnen vormen voor betrokkenen. Melding bij AP/verzoeker niet nodig.	- Bericht van onterechte ontvanger gekregen dat e-mail verwijderd is. - de onterecht geadresseerde is verzocht om e-mailbericht te vernietigen. In afwachting van reactie.
10	27-8-2021	Niet gemeld aan AP	Vermoedelijk datalek, e-mail naar verkeerde geadresseerde	Twee e-mails naar DUO gestuurd naar verkeerd emailadres (binnen DUO). E-mail bevat naam en adresgegevens van verzoeker en naam/contactgegevens van onderzoeker.	- Navraag bij DUO wat er met de foutief afgeleverde e-mails gebeurt. - Controle gedaan op contactgegevens in Verseon en Kennisbank. E-mailadres staat daar goed.
11	10-8-2021	Niet gemeld aan AP	Datalek: verkeerde geadresseerde	Onjuist e-mailadres gebruikt met naam van andere verzoeker en inhoud dat wij kijken naar afgeronde klachtenprocedures en niet meer zullen reageren op doorgestuurde berichten. Betrokken persoonsgegevens: Naam verzoeker	Verzoek om geadresseerde te vragen het e-mailbericht te vernietigen.
12	8-7-2021	Niet gemeld aan AP	Verzoeker straatnaam genoemd van naamgenoot	Bij telefonisch nagaan van NAW-gegevens van een verzoeker, werd uit eigen beweging de (verkeerde) straatnaam genoemd. Verzoeker weet nu mogelijk dat er een naamgenoot is met klacht bij de No.	Bij constatering van meerdere resultaten n.a.v. zoeken op persoonsgegevens, moet om meer informatie gevraagd worden (wat is de straatnaam?) in plaats van aangeboden worden (woont u op...?).

13	15-6-2021	Niet gemeld aan AP	Datalek: E-mail verstuurd naar verkeerde afzender	Persvraag doorgestuurd naar collega's en daarbij een verkeerd emailadres opgenomen van een extern persoon.	Emailbericht is verwijderd door onterechte ontvanger.
14	2-6-2021	Niet gemeld aan AP	Datalek: e-mail naar externe verzoeker i.p.v. interne medewerker	Email bevat namen van een paar collega's en een naam van een contactpersoon bij de belastingdienst en een telefoonnummer. Geen bijzondere of gevoelige informatie.	Verkeerde ontvanger heeft gemeld dat email onterecht bij hem is terechtgekomen. Ontvanger vragen om mail te verwijderen/vernietigen.
15	31-5-2021	Niet gemeld aan AP	Datalek: brief verstuurd naar oud adres	Brief is verstuurd naar een adres waar ontvanger niet langer woonachtig is.	- anonieme brief wordt niet gepubliceerd op internet - onterechte ontvangers worden per post verzocht om de brief te vernietigen of retourneren.
16	23-5-2021	Niet gemeld aan AP	Datalek: e-mails verstuurd naar verkeerd e-mailadres	2 e-mails met informatie over een dossier verstuurd naar verkeerd e-mailadres. E-mails zijn afgeleverd. De persoonsgegevens in de e-mails betreffen: naam verzoeker en dossiernummer en naam van wethouder. Verder geen gevoelige gegevens.	Verkeerde ontvanger wordt verzocht om de e-mails te vernietigen. Reactie gekregen van de onterechte ontvanger met de boodschap dat hij de mail heeft verwijderd.
17	11-5-2021	Gemeld aan AP door verwerker, niet betrokkene	Datalek testdatabase NoHow	In de database bevinden accountgegevens van CMS en mogelijk persoonsgegevens.	Maatregelen verwerker: - De beveiliging van onze servers is inmiddels grotendeels nagelopen, zijn rechten beperkt en is er waar nodig rechten extra aangescherpt. - De betreffende server wordt zo snel mogelijk uit gefaseerd en de data wordt alleen overgenomen als dit echt nodig is. - Password CMS accounts productieomgeving zijn aangepast.
18	24-3-2021	Niet gemeld aan AP	Beveiligingsincident	Caching internetpagina, bij invullen bestelformulier mogelijk persoonsgegevens van vorige invuller	Bug in systeem is opgelost.
19	31-12-2020	Niet gemeld aan AP	Datalek: mail naar verkeerde afzender	Mail en pdf-document. Bevat alleen emailadressen van behandelaar en	Onterechte ontvanger is verzocht om mail te verwijderen.

				collega en medewerker bij de belastingdienst. Mail is verstuurd naar een verkeerd persoon binnen de belastingdienst.	
20	29-12-2020	Niet gemeld aan AP	Datalek: verkeerde geadresseerde gemaild	Mail voor interne collega is naar verzoeker met zelfde voornaam gegaan.	Onterechte ontvanger heeft de mail verwijderd.
21	4-12-2020	Niet gemeld aan AP	Datalek: brief verstuurd naar partner van geadresseerde.	Brief bevat NAW-gegevens, verder geen gevoelige persoonsgegevens. Ontvanger is man van de beoogde ontvanger.	Ontvanger heeft bevestigd het bericht te vernietigen.
22	30-11-2020	Niet gemeld aan AP	E-mail naar verkeerde medewerker, met zelfde voornaam, verstuurd	Betreft: gegevens van een medewerker	Onterechte ontvanger heeft aangegeven de mail te vernietigen
23	19-11-2020	Niet gemeld aan AP	Datalek: VVB naar verkeerde ontvanger. Typefout in e-mailadres	Document bevat adresgegevens van betrokkene en gegevens van onderzoeker.	Onrechtmatige ontvanger heeft contact opgenomen om te melden dat bericht onterecht ontvangen is. Op verzoek is deze vernietigd.
24	19-10-2020	Niet gemeld aan AP	Datalek: Mail naar verkeerde persoon buiten de organisatie gestuurd	De mail bevatte alleen 6 e-mailadressen van medewerkers geen verdere persoonsgegevens.	Verzoek aan onterechte ontvanger. Ontvanger heeft direct gereageerd en mail verwijderd.
25	9-10-2020	Niet gemeld aan AP	Datalek: verkeerde klacht als bijlage meegestuurd aan de huurcommissie.	De bijlage bij de doorgestuurde e-mail betreft de klacht zoals deze bij de No is ingediend. Hierin staan de NAW-gegevens, het telefoonnummer en het e-mailadres van andere verzoeker dan van de doorgestuurde e-mail.	Huurcommissie heeft een reactie gestuurd met daarin de melding van een datalek en bericht dat de bijlage is vernietigd.
26	23-9-2020	Niet gemeld aan AP	Datalek: e-mail naar verkeerde verzoeker	: in de mail staan de naam van de verzoeker en het dossiernummer. Verder een algemene opsomming van het verzoek. De persoon is niet direct herleidbaar en het bericht bevat geen gevoelige info.	De verkeerd geadresseerde is verzocht de mail te verwijderen en excuus is aangeboden. Verder geen actie nodig.
27	3-9-2020	Niet gemeld aan AP	Reactie op klacht per post naar verkeerde adres verstuurd.	De brief bevat geen gevoelige gegevens behalve dossiernummer, NAW-gegevens van verzoeker en korte samenvatting van de klacht.	- Adres aanpassen in systeem - Brief opnieuw versturen (wellicht met excuses) naar juiste adres.

28	20-7-2020	Niet gemeld aan AP	Datalek: Eindbrief dossier verstuurd naar verkeerde ontvanger.	Hoewel de brief de naam en adresgegevens van de betrokkene bevat, bevat de brief verder geen bijzondere of gevoelige informatie wat in het nadeel van de verzoeker zou kunnen werken.	- De betrokkene die de brief had moeten ontvangen is op de hoogte gesteld en excuus aangeboden - De verkeerde ontvanger is verzocht het stuk te retourneren of vernietigen - De klachtbehandelaar past werkwijze aan om dergelijke fout in de toekomst te voorkomen. (bestaande brief gebruiken voor een andere klacht en bepaalde gegevens niet aanpassen)
29	16-7-2020	Niet gemeld aan AP	Datalek: mail verstuurd met geadresseerden zichtbaar voor iedereen.	Geadresseerden waren niet opgenomen in de bcc. Er is voornamelijk gebruik gemaakt van groepsadressen waardoor er feitelijk niet veel adressen openbaar zijn gemaakt voor de anderen. Het gaat om de telegraaf en een aantal groepen van de No. De inhoud van het bericht betreft een column voor de telegraaf.	Geen verdere actie nodig.
30	16-6-2020	Niet gemeld aan AP	Datalek: e-mail naar verkeerd (oud) adres gestuurd.	E-mail bevat alleen naam van de verzoeker, dossiernummer en gegevens van klachtbehandelaar.	Er is contact opgenomen met de verzoeker. Geen verdere actie nodig. E-mailadres in het zaaksysteem aangepast.
31	9-6-2020	Niet gemeld aan AP	Datalek; gepubliceerde rapportbrief met naam derde er nog in	In een gepubliceerde rapportbrief is de naam van een derde blijven staan. Deze persoon is niet de verzoeker en speelt geen directe rol in het dossier.	- De betrokkene wordt op de hoogte gesteld en excuus aangeboden door onderzoeker. - Er wordt onderzocht of er naast vakstudienieuws nog andere partijen zijn die de rapportbrief gebruiken/publiceren. - Proces van anonimiseren wordt nader bekeken ter verbetering.
32	28-5-2020	Niet gemeld aan AP	Datalek: klacht van een andere verzoeker meegestuurd met terugbelverzoek	Er was een terugbelverzoek naar verzoeker gemaild. Onder het terugbelverzoek zat een klacht van een andere verzoeker. De verzoeker van het terugbelverzoek heeft aangegeven dat dit een andere klacht is. De klachtbeschrijving bevat naast een omschrijving de NAW-gegevens van een verzoeker	Reactie met het verzoek de e-mail te verwijderen.

33	20-5-2020	Niet gemeld aan AP	Datalek: verslag van braingain verstuurd naar medewerkers en verkeerd extern adres.	Verslag zelf bevat geen persoonsgegevens, maar emailadressen van 5 medewerkers zijn wel naar verkeerde derde gegaan.	De ontvanger is verzocht om het bericht te verwijderen, verder geen actie nodig.
34	8-5-2020	Niet gemeld aan AP	Datalek: naam genoemd in rapport op website	Het betreft een bijlage bij een rapportbrief op de website. De brief was niet volledig geanonimiseerd.	- Gegevens in de brief geanonimiseerd - Anonimiseer procedure bekijken, zien of verbeteringen mogelijk zijn
35	10-4-2020	Niet gemeld aan AP	Datalek: p-direkt vraag verstuurd via mail waarbij per ongeluk een verkeerde geadresseerde in is opgenomen.	Schaal en naam medewerker is gedeeld.	Geen ernstige gevolgen en geen maatregelen nodig.
36	6-3-2020	Geen datalek	Geen datalek: e-mailadres blijkt niet te bestaan	E-mail naar een verkeerd e-mailadres gestuurd	Mail is niet afgeleverd. Geen verdere actie nodig.
37	24-2-2020	Gemeld aan AP en betrokkene	Datalek: gegevens naar verkeerde persoon	Twee brieven zijn naar verkeerde adres (verkeerd huisnr) van vz gestuurd in 2019	- Datalek is gemeld aan betrokkenen - Verzocht aan onterechte ontvangers de post te retourneren of vernietigen, als dat al niet gebeurd is. - Intern besproken met verzoek om erg goed op te letten bij het verzenden van stukken
38	20-2-2020	Niet gemeld aan AP	Datalek: e-mail verstuurd naar verkeerde geadresseerde.	E-mail bevat naam, e-mailadres en dossiernummer van behandelaar en verzoeker.	Verzoek aan onterechte ontvanger om e-mail te verwijderen.
39	11-2-2020	Niet gemeld aan AP	Datalek: e-mail verzonden naar verkeerde geadresseerde.	E-mail bericht naar verkeerde geadresseerde, bevat dossiernummer en contactgegevens van onderzoeker.	Verzoek aan onterechte ontvanger om e-mail te verwijderen.

Standaardmelding van een datalek aan betrokkene(n): verspreiding of inzage

Onderstaande tekst kan worden gebruikt bij het melden van een datalek aan betrokkene(n).

Geachte [heer/mevrouw] [achternaam],

--onderstaande paragraaf gebruiken indien gebeld is---
Op [datum] heb ik u gebeld en laten weten dat uw persoonsgegevens via ons per ongeluk [bij derden terecht zijn gekomen [en/of] mogelijk door derden zijn ingezien]. Wij vinden dit erg vervelend en bieden hier nogmaals onze excuses voor aan. Met deze brief bevestig ik wat wij tijdens ons telefoongesprek besproken hebben.

--onderstaande paragraaf gebruiken indien NIET gebeld is---
Wij hebben geconstateerd dat uw persoonsgegevens via ons per ongeluk [bij derden terecht zijn gekomen [en/of] mogelijk door derden zijn ingezien]. Wij vinden dit erg vervelend en bieden hiervoor allereerst onze excuses aan. In deze brief leest u om welke gegevens het gaat en wie hiertoe toegang gekregen heeft. Ook informeren wij u over de maatregelen die u zelf kunt nemen om de gevolgen te beperken.

Wat is er gebeurd?
Wij hebben geconstateerd dat uw gegevens omstreeks [datum]

[Opties:
- [zijn ingezien door personen of instanties die hiertoe geen toegang mochten hebben]. [*licht toe om welke personen/instanties het gaat en wat er is gebeurd*]
- [aan de verkeerde persoon zijn toegestuurd, namelijk]: [uw leidinggevende / een andere burger / uw echtgeno(o)t(e) / [naam overheidsinstantie]. [*Licht toe wat er is gebeurd*]
- [door iemand zijn gekopieerd zonder uw toestemming]. [*Licht toe wat er is gebeurd*]
- [tijdens vervoer zijn gestolen of verloren]. [*Licht toe wat er is gebeurd*]
- [tijdens een digitale inbraak zijn ontvreemd]. [*Licht toe wat er is gebeurd*]

Het gaat om de volgende persoonsgegevens:
[opsomming]

Wat betekent dit voor u?
Doordat uw persoonsgegevens terecht zijn gekomen bij anderen, loopt u mogelijk de kans op

[Opties:
- [stigmatisering of uitsluiting van] [toelichting]
- [schade aan de gezondheid door] [toelichting]

- [(identiteits)fraude waarbij iemand uw persoonsgegevens misbruikt. Denk bijvoorbeeld aan het afsluiten van abonnementen op uw naam of het doen van aankopen.]
- [(identiteits)fraude waarbij iemand uw persoonsgegevens en/of een kopie van uw identiteitsbewijs misbruikt. Denk bijvoorbeeld aan het afsluiten van abonnementen op uw naam of het doen van aankopen.]
- [spam of phishing. In dat geval vraagt iemand u om informatie te geven of een bepaalde actie uit te voeren. Die persoon geeft u een vals gevoel van vertrouwen door uw persoonlijke gegevens te noemen en zich voor te doen als een bekende of organisatie waar u zaken mee doet.]
- [Overig] [Toelichting]

Wat hebben wij gedaan?
[Wij hebben de onterechte ontvanger van uw persoonsgegevens verzocht uw persoonsgegevens direct te vernietigen of aan ons retour te zenden.]

Wat kunt u doen?
Wij adviseren u de komende periode alert te zijn op misbruik van uw persoonsgegevens.

[Opties:

- Als u vermoedt dat iemand anders uw identiteit gebruikt, doe dan aangifte bij de politie.
- Houd uw bankafschriften in de gaten om misbruik of verdachte betalingen te kunnen constateren. Meld misbruik altijd direct bij uw bank.
- Ga nooit in op e-mail berichten of telefoongesprekken waarin iemand om uw persoonlijke gegevens vraagt. Bij e-mail: klik nooit op links in een verdacht e-mailbericht. Ga er niet op in als iemand u vraagt een actie uit te voeren zoals het downloaden en installeren van software op uw computer. Vraag bij telefonische verzoeken de naam van de medewerker en bel zelf de organisatie terug voordat u verder gaat.
- [eventuele specifieke zaken]

Meer informatie
Op de website van de Rijksoverheid vindt u meer informatie over identiteitsfraude via deze link: https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude. Meer informatie over online fraude vindt u hier:
https://www.rijksoverheid.nl/onderwerpen/cybercrime/vraag-en-antwoord/phishing

Hebt u nog vragen?
Hebt u over deze brief nog vragen, neem dan contact op met [naam]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer]

Met vriendelijke groet,

[naam medewerker]

Standaardmelding van een datalek aan betrokkene(n): wijziging

Onderstaande tekst kan worden gebruikt bij het melden van een datalek aan betrokkene(n).

Geachte [heer/mevrouw] [achternaam],

--onderstaande paragraaf gebruiken indien gebeld is---
Op [datum] heb ik u gebeld en laten weten dat uw persoonsgegevens via ons per ongeluk onbedoeld zijn gewijzigd en deze onjuiste gegevens aan andere organisaties zijn verstrekt. Wij vinden dit erg vervelend en bieden hier nogmaals onze excuses voor aan. Met deze brief bevestig ik wat wij tijdens ons telefoongesprek besproken hebben.

--onderstaande paragraaf gebruiken indien NIET gebeld is---
Wij hebben geconstateerd dat uw persoonsgegevens via ons per ongeluk onbedoeld zijn gewijzigd en deze onjuiste gegevens aan andere organisaties zijn verstrekt. Wij vinden dit erg vervelend en bieden u hiervoor allereerst onze excuses aan. In deze brief leest u om welke gegevens het gaat en aan wie deze zijn verstrekt. Ook informeren wij u over de maatregelen die u zelf kunt nemen om de gevolgen te beperken.

Wat is er gebeurd?
Wij hebben geconstateerd dat uw gegevens omstreeks [datum]

[Opties:
- [onbedoeld in onze administratie zijn gewijzigd door één van onze medewerkers] [*licht toe om welke personen/instanties het gaat en wat er is gebeurd*]
- [onbedoeld in onze administratie zijn gewijzigd door een derde] [*licht toe om welke personen/instanties het gaat en wat er is gebeurd*]

Het gaat om de volgende persoonsgegevens:
[opsomming]

De onjuiste gegevens zijn tijdens de behandeling van uw klacht verstrekt aan [naam organisatie(s)].

Wat zijn de gevolgen voor u?
Doordat wij onjuiste gegevens over hebben doorgegeven loopt u mogelijk een verhoogd risico op
[Opties:
- [stigmatisering of uitsluiting van] [toelichting]
- [schade aan de gezondheid door] [toelichting]
- [Overig] [Toelichting]

Wat hebben wij gedaan?
Wij hebben aan de ontvanger van uw persoonsgegevens geïnformeerd dat wij onjuiste gegevens hebben verstrekt en hem verzocht deze te corrigeren.

Wat kunt u doen?
Wij adviseren u berichten van [naam organisaties] goed te controleren om te zien of hierop onjuiste gegevens staan. Neem in dat geval contact op met [naam organisatie]. [eventueel concrete aanbevelingen toevoegen]

Meer informatie
Hebt u over deze brief nog vragen, neem dan contact op met [naam]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer]

Met vriendelijke groet,

[naam medewerker]

Standaardmelding van een datalek aan betrokkene(n): verlies of vernietiging zonder reservekopie

Onderstaande tekst kan worden gebruikt bij het melden van een datalek aan betrokkene(n).

Geachte [heer/mevrouw] [achternaam],

--onderstaande paragraaf gebruiken indien gebeld is---
Op [datum] heb ik u gebeld en laten weten dat [wij uw gegevens per ongeluk uit onze verwijderd hebben] / [uw gegevens in onze administratie verloren zijn gegaan]. Wij vinden dit erg vervelend en bieden hier nogmaals onze excuses voor aan. Met deze brief bevestig ik wat wij tijdens ons telefoongesprek besproken hebben.

--onderstaande paragraaf gebruiken indien NIET gebeld is---
Wij hebben geconstateerd dat [wij uw gegevens per ongeluk uit onze verwijderd hebben] / [uw gegevens in onze administratie verloren zijn gegaan]. Wij vinden dit erg vervelend en bieden u hiervoor allereerst onze excuses aan. In deze brief leest u om welke gegevens het gaat.

Om welke gegevens gaat het?
De volgende gegevens hebben wij niet meer van u:

- [opsomming]

Wat vragen wij van u?
Wij hebben bovenstaande gegevens niet meer van u. Daarom vragen wij u ons deze gegevens opnieuw te geven en/of op te vragen bij de betrokken instantie(s). U kunt hiervoor contact opnemen met uw klachtbehandelaar [naam klachtbehandelaar]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer].

Wat betekent dit voor u?
Doordat een deel van uw gegevens in onze administratie verloren is gegaan, [concreet maken van consequenties].

Hebt u nog vragen?
Hebt u over deze brief nog vragen, neem dan contact op met [naam]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer]

Met vriendelijke groet,

[naam medewerker]

Standaardverzoek aan onterechte ontvanger: algemeen, poststuk

Onderstaande tekst kan worden gebruikt om een onterechte ontvanger te verzoeken stukken te retourneren of te vernietigen.

Geachte [heer/mevrouw] [achternaam],

Volgens onze gegevens heeft u stukken ontvangen over een ander persoon waarmee de Nationale ombudsman contact heeft (gehad). Dit was niet de bedoeling en is het gevolg van een menselijke fout.

Het gaat om de volgende stukken die wij op [datum] per post aan u gestuurd hebben:

- [opsomming]

Wat vragen wij van u?
Aangezien deze stukken niet voor u bestemd zijn, verzoeken wij u dringend deze zo snel mogelijk aan ons terug te sturen. U kunt alle stukken in een gesloten enveloppe aan ons terugsturen via ons gratis postadres (een postzegel is niet nodig):

Nationale ombudsman
t.a.v. [naam]
Antwoordnummer 10870
2501 WB Den Haag

Ook vragen wij u om alle informatie vertrouwelijk te behandelen en niet met anderen te delen. Het delen van informatie uit de stukken die u heeft ontvangen, kan schade opleveren voor de persoon voor wie deze stukken bedoeld zijn.

Mocht u de stukken inmiddels niet meer in bezit hebben, dan vragen wij u contact op te nemen met [naam]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer]

Hebt u nog vragen?
Wij vinden deze gebeurtenis zeer vervelend en bieden u hiervoor onze excuses aan. Ook willen wij u vast danken voor uw moeite en medewerking. Hebt u over deze brief nog vragen, neem dan contact op met [naam]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer]

Met vriendelijke groet,

[naam medewerker]

Standaardverzoek aan onterechte ontvanger: algemeen, e-mail

Onderstaande tekst kan worden gebruikt om een onterechte ontvanger te verzoeken stukken te retourneren of te vernietigen.

Geachte [heer/mevrouw] [achternaam],

Volgens onze gegevens heeft u stukken ontvangen over een ander persoon waarmee de Nationale ombudsman contact heeft (gehad). Dit was niet de bedoeling en is het gevolg van een menselijke fout.

Het gaat om de volgende stukken die wij op [datum] per e-mail aan u gestuurd hebben:

- [opsomming]

Wat vragen wij van u?
Aangezien deze gegevens niet voor u bestemd zijn, verzoeken wij u dringend deze gegevens zo snel mogelijk te verwijderen. Wilt u ons zo snel als mogelijk berichten wanneer u de e-mail en bijlagen verwijderd heeft? Ook als u deze gegevens al eerder verwijderd heeft. U kunt ons dit laten weten door te antwoorden op deze e-mail.

Daarnaast vragen wij u om alle informatie vertrouwelijk te behandelen en niet met anderen te delen. Het delen van informatie uit de stukken die u heeft ontvangen, kan schade opleveren voor de persoon voor wie deze stukken bedoeld zijn.

Inmiddels hebben wij de persoon voor wie de stukken bedoeld waren over deze verzendfout geïnformeerd.

Hebt u nog vragen?
Wij vinden deze gebeurtenis zeer vervelend en bieden hiervoor onze excuses aan. Ook willen wij u vast danken voor uw moeite en medewerking. Hebt u over deze brief nog vragen, neem dan contact op met [naam]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer]

Met vriendelijke groet,

[naam medewerker]

Standaardherinnering aan onterechte ontvanger: algemeen, poststuk

Onderstaande tekst kan worden gebruikt om een onterechte ontvanger te verzoeken stukken te retourneren of te vernietigen.

Geachte [heer/mevrouw] [achternaam],

Op [datum] hebben wij u laten weten dat u stukken van ons heeft ontvangen, die voor een ander persoon bedoeld waren. We hebben u verzocht deze stukken aan ons terug te sturen. Wij hebben echter nog geen reactie van u ontvangen. Wij vragen u met deze brief opnieuw hierom.

Het gaat om de volgende stukken die wij op [datum] per post aan u gestuurd hebben:

- [opsomming]

Wat vragen wij van u?
Wij verzoeken u dringend om de stukken binnen 10 dagen terug te sturen.
U kunt alle stukken in een gesloten enveloppe aan ons terugsturen via ons gratis postadres (een postzegel is niet nodig):

Nationale ombudsman
t.a.v. [naam]
Antwoordnummer 10870
2501 WB Den Haag

Ook vragen wij u om alle informatie vertrouwelijk te behandelen en niet met anderen te delen. Het delen van informatie uit de stukken die u heeft ontvangen, kan schade opleveren voor de persoon voor wie deze stukken bedoeld zijn.

Mocht u bovenstaande stukken inmiddels niet meer in bezit hebben, dan vragen wij u contact op te nemen met [naam]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer]

Wij hebben de persoon voor wie de stukken bedoeld waren over de verzendfout geïnformeerd.

Hebt u nog vragen?
Wij vinden deze gebeurtenis zeer vervelend en bieden u hiervoor onze excuses aan. Ook willen wij u vast danken voor uw moeite en medewerking. Hebt u over deze brief nog vragen, neem dan contact op met [naam]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer]

Met vriendelijke groet,
[naam medewerker]

Standaardherinnering aan onterechte ontvanger: algemeen, e-mail

Onderstaande tekst kan worden gebruikt om een onterechte ontvanger te verzoeken stukken te retourneren of te vernietigen.

Geachte [heer/mevrouw] [achternaam],

Op [datum] hebben wij u laten weten dat u stukken van ons via e-mail heeft ontvangen, die voor een ander persoon bedoeld waren. We hebben u verzocht deze e-mail en bijlagen te verwijderen en het ons te laten weten als dit gebeurd was. Wij hebben echter nog geen reactie van u ontvangen. Wij vragen u met deze brief opnieuw hierom.

Het gaat om de volgende stukken die wij op [datum] per e-mail aan u gestuurd hebben:

- [opsomming]

Wat vragen wij van u?
Aangezien deze gegevens niet voor u bestemd zijn, verzoeken wij u dringend deze gegevens zo snel mogelijk te verwijderen. Wilt u ons zo snel als mogelijk berichten wanneer u de e-mail en bijlagen verwijderd heeft? Ook als u deze gegevens al eerder verwijderd heeft. U kunt ons dit laten weten door te antwoorden op deze e-mail.

Wij vragen u vriendelijk maar dringend om binnen 10 dagen aan ons te bevestigen dat de e-mail en bijlagen verwijderd zijn. Ook als u deze gegevens al eerder verwijderd heeft. U kunt ons dit laten weten door te antwoorden op deze e-mail.

Daarnaast vragen wij u om alle informatie vertrouwelijk te behandelen en niet met anderen te delen. Het delen van informatie uit de stukken die u heeft ontvangen, kan schade opleveren voor de persoon voor wie deze stukken bedoeld zijn.

Wij hebben zowel de persoon voor wie de stukken bedoeld over de verzendfout geïnformeerd.

Hebt u nog vragen?
Wij vinden deze gebeurtenis zeer vervelend en bieden u hiervoor onze excuses aan. Ook willen wij u vast danken voor uw moeite en medewerking. Hebt u over deze brief nog vragen, neem dan contact op met [naam]. U kunt [hem/haar] op [werkdagen] bereiken via telefoonnummer [telefoonnummer]

Met vriendelijke groet,

[naam medewerker]

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	25-02-2020 13:37:00
Uniek nummer	[redacted]

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	11111111

Naam van het bedrijf of de organisatie	Nationale ombudsman
Adres	Bezuidenhoutseweg 151
Postcode	2594AG
Plaats	Den haag
In welke sector is de organisatie of het bedrijf actief?	Openbaar bestuur - Rijksoverheid

Wie meldt het datalek?

Naam	[redacted]
Functie	Controller
E-mailadres	[redacted]@nationaleombudsman.nl
Telefoonnummer	070-[redacted]
Tweede telefoonnummer	06-[redacted]

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Nee
Naam contactpersoon	[redacted]
Functie contactpersoon	FG
E-mailadres contactpersoon	avg@nationaleombudsman.nl
Telefoonnummer contactpersoon	+31 70[redacted]
Tweede telefoonnummer contactpersoon	06-[redacted]

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Ja, namelijk:
Naam van de andere organisatie die betrokken was bij de inbreuk	Belastingdienst

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?
in de informatie is ook een besluit van de Belastingdienst/toeslagen meegezonden.

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	26-04-2019
Startdatum van de periode waarbinnen de inbreuk was	27-04-2019
Duurt de inbreuk op dit moment nog voort?	Ja
Wanneer werd de inbreuk ontdekt?	24-02-2020

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Brief aan burger met een klacht met hierin gegevens van Toeslagen Belastingdienst en de gegevens van zijn kinderen zijn verzonden naar een foutief adres.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Ja
Burgerservicenummer (BSN)	Nee
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Nee
Financiële gegevens	Ja
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Ja
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee
Onbekend / anders, namelijk:	dossiernummer

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee

Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	2

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Nee
Leerlingen of studenten	Nee
Patiënten	Nee
Minderjarigen	Ja
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
het betreffen de gegevens van de verzoeker en vier kinderen

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	5
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	5

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich	Nee

voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Ja
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Ja
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Nee

Identiteitsdiefstal of -fraude	Ja
Financiële verliezen	Nee
Reputatieschade	Ja
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Ja
Wanneer heeft u het datalek gemeld aan de betrokkenen?	25-02-2020

Wat is de inhoud van de melding aan de betrokkenen?
abusievelijk is vorig jaar bij de verzending van twee brieven aan u een verkeerd huisnummer gebruikt, wij zullen contact opnemen met de bewoners van dat huisadres en verzoeken de post te retourneren of vernietigen als dat al niet gebeurd is. en zullen verzoeker op de hoogte houden hiervan. Intern hebben wij dit datalek uitgebreid besproken, zodat

hier weer aandacht voor is en kan datalek worden voorkomen. ondertussen zijn uw gegevens wel correct in onze systemen doorgevoerd. Ook is hier melding van gemaakt bij het AP.

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	2
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	per brief en mail

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Datalek is intern in het team besproken, met het verzoek om erg goed op te letten bij het verzenden van stukken en om juiste gegevens te gebruiken. contactgegevens zijn aangepast

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere	Nee

meldplichten, of gaat u dat nog doen?	

9. Overig

Is naar uw mening deze melding compleet?	Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig

doc 4

Protocol datalekken

Nationale Ombudsman

Versiebeheer

Naam document	Protocol Datalekken
Verantwoordelijke	
Auteur	No
Review	Ilionx
Versienummer	1.0
Datum eerste versie	
Laatst bijgewerkt	1 juni 2021

Wijzigingen			
Datum	**Versie**	**Door**	**Wijzigingen**

Protocol meldplicht datalekken

1. Inleiding

Iedereen heeft recht op privacy en wil dat er zorgvuldig wordt omgegaan met zijn of haar persoonsgegevens. De regels hiervoor staan in de Algemene Verordening Gegevensbescherming (AVG). Hierin staat onder meer dat de verwerkte persoonsgegevens beveiligd moeten worden tegen verlies en tegen onrechtmatige verwerking (artikel 32 AVG). Indien een datalek leidt tot risico's ten aanzien van rechten en vrijheden van natuurlijke personen, dient het datalek gemeld te worden aan de verantwoordelijke autoriteit (artikel 33 AVG). In Nederland is dit de Autoriteit Persoonsgegevens (AP). Het datalek moet in sommige gevallen ook worden gemeld aan de betrokkene (artikel 34 AVG). Ieder datalek wordt door de Nationale ombudsman (No) geregistreerd, beoordeeld en eventueel gemeld aan de Autoriteit Persoonsgegevens en de betrokkene(n) waarvan de persoonsgegevens zijn gelekt.Dit protocol beschrijft de procedure die binnen de No wordt gevolgd om te voldoen aan artikel 33 en 34 AVG.

Definitie datalek
In artikel 4 lid 12 AVG wordt ‘een inbreuk in verband met de persoonsgegevens’ (datalek) gedefinieerd als: ‘een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens’. Bij een datalek moet je bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of een inbraak door een hacker. Indien het enkel gaat om een zwakke plek in de beveiliging, is er sprake van een beveiligingslek en niet van een datalek. In het geval van een beveiligingslek hoeft er geen melding te worden gedaan bij de AP. In bijlage 2 zijn diverse voorbeelden van datalekken opgenomen.

2. Melding datalek binnen de No

Datalekken worden als volgt gemeld:

a. Melding vanuit de organisatie
Een geconstateerd datalek binnen de organisatie wordt overeenkomstig dit protocol gemeld bij de Functionaris gegevensbescherming (FG) via het ‘formulier melding datalek’ dat via intranet beschikbaar is. Het formulier wordt zonder bijlagen aan een datalek melding in TopDesk toegevoegd. Iedere medewerker meldt een datalek direct, maar in ieder geval binnen 24 uur na het ontdekken van het datalek. De medewerker informeert tevens zijn manager over deze melding. Datalekken worden binnen de No ook gemeld indien tijdens een beveiligingsincident wordt vastgesteld dat er ook sprake is van een datalek.

b. Melding vanuit een verwerker
Met verwerkers van persoonsgegevens worden in de verwerkersovereenkomst schriftelijke afspraken gemaakt over de melding van datalekken. Een verwerker meldt elk incident binnen 24 uur na het ontdekken van het datalek aan de FG van de No.

c. Melding vanuit derden
Indien derden - zoals burgers, instanties of ondernemingen - een datalek bij de Nationale ombudsman melden, dan neemt de FG telefonisch contact op om het (vermoedelijke) datalek te bespreken. Tijdens het gesprek vult de FG het ‘formulier melding datalekken’ in.

3. Registratie van datalekken

Alle datalekken worden geregistreerd in TopDesk. Ook opvolging en rapportages zijn met behulp van TopDesk ingericht. In TopDesk is hiervoor voor incidenten de categorie “Datalek” beschikbaar.

Een datalek kan op twee manieren worden gemeld:

1. Als een medewerker rechtstreeks een datalek meldt (bijvoorbeeld via [redacted]@nationaleombudsman.nl), wordt deze door de FG geregistreerd in TopDesk.

2. Als een beveiligingsincident wordt gemeld waarbij persoonsgegevens betrokken zijn, wordt de FG geïnformeerd en deze voert een korte toets uit waarmee wordt bepaald of dit mogelijk een datalek volgens de AVG betreft. Indien dit niet het geval is, dan wordt het beveiligingsincident normaal afgehandeld overeenkomstig het incidentmanagementprotocol.

   Als het beveiligingsincident wel een datalek is, maakt de medewerker een nieuwe (tweede) melding aan in Topdesk, met de categorie “Datalek” en subcategorie “Vermoedelijk”. (De subcategorie wordt later in het proces door de FG gewijzigd). De oorspronkelijke melding blijft op naam van de juiste behandelaar staan, terwijl de tweede melding over het datalek standaard aan de FG wordt toegewezen.

Hierna ontvangt de melder automatisch de volgende e-mail vanuit Topdesk, met als bijlage het ‘formulier melding datalek’:

Onderwerp: Datalek melding met nr. [meldingnummer] is aangemaakt.

Beste collega,

Je hebt een datalek melding geregistreerd in TOPdesk.

Vul het bijgevoegde formulier "melding datalek" zo snel mogelijk in en upload het document vervolgens in de melding.

Klik op de volgende link om de melding in TOPdesk te bekijken: *<URL naar melding in TOPdesk SelfServiceDesk gedeelte>*

Via de link die in de e-mail is opgenomen kan de melder in Topdesk het datalek blijven volgen.

De leden van de distributiegroep [redacted]@nationaleombudsman.nl ontvangt van iedere melding in Topdesk een notificatie per e-mail:

Onderwerp: Datalek melding met nr. [Meldingnummer] is aangemaakt.

Beste collega, Er is een datalek melding geregistreerd met nummer I <nummer>.

Klik op de volgende link om de melding in TOPdesk te bekijken: *<URL naar melding in TOPdesk behandelaarsgedeelte>*

In de distributiegroep [redacted]@nationaleombudsman.nl zijn in ieder geval de FG, CISO en één of meer AVG vertegenwoordigers opgenomen.

De melder vult het formulier in en stuurt dit naar de distributiegroep [redacted]@nationaleombudsman.nl. De FG is verantwoordelijk voor de volledige en correcte dossiervorming in Bureaudok (Verseon).

Alle relevante informatie over het datalek wordt in TopDesk geregistreerd, waaronder:

- de kenmerken van het beveiligingsincident en de toetsing of dit een datalek betreft
- de beoordeling of een melding aan betrokkene(n) moet plaatsvinden

De documenten worden opgeslagen in Bureaudok. Dit dossier wordt gekoppeld aan de melding in Topdesk. In Bureaudok wordt opgenomen:

- het 'Formulier melding datalek' waarin de kenmerken van het datalek zijn opgenomen
- de melding aan de Autoriteit persoonsgegevens
- indien van toepassing: de melding aan betrokkene(n)
- indien van toepassing: communicatie naar onterechte ontvangers van persoonsgegevens

In TopDesk en Bureaudok worden nooit inhoudelijke stukken / de gelekte gegevens opgenomen in het datalek dossier, dit om te voorkomen dat via deze weg persoonsgegevens worden verspreid.

4. Werkwijze ten behoeve van externe melding

De FG beoordeelt of er sprake is van een datalek met meldplicht. Dit wordt beoordeeld aan de hand van artikel 33 en 34 AVG, de beleidsregels meldplicht datalekken van de Autoriteit persoonsgegevens en de in bijlage 2 opgenomen criteria.

In geval van een datalek dat extern gemeld moet worden, informeert de FG de CISO en de directie.

a. Melding aan de Autoriteit persoonsgegevens

Een datalek moet ingevolge artikel 33 AVG zonder onredelijke vertraging en indien mogelijk uiterlijk binnen 72 uur nadat er kennis van is genomen worden gemeld aan de Autoriteit persoonsgegevens, tenzij onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt.

De FG of diens vervanger meldt het datalek aan de Autoriteit persoonsgegevens. De melding zal plaatsvinden binnen 72 uur na het ontdekken van het datalek en via het daarvoor beschikbaar gestelde webformulier van de Autoriteit persoonsgegevens. Deze is te vinden op: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

b. Melding aan betrokkene(n)

Een datalek wordt ingevolge art 34 AVG onverwijld gemeld aan betrokkene indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene.

De FG of diens vervanger draagt zorg voor het melden van het datalek aan de betrokkene(n). De melding bevat op grond van artikel 34 lid 2 AVG in ieder geval - in duidelijke en eenvoudige taal - de aard van de inbreuk, de naam en contactgegevens van de FG, waar de betrokkene meer informatie over de inbreuk kan krijgen, de waarschijnlijke gevolgen van de inbreuk en de maatregelen die de Nationale ombudsman heeft voorgesteld of genomen om de negatieve gevolgen van de inbreuk te beperken.

De melding aan een betrokkene wordt overeenkomstig de 'standaardreacties datalekken' in kennisbank IV gedaan.

c. Verzoek aan onterechte ontvanger

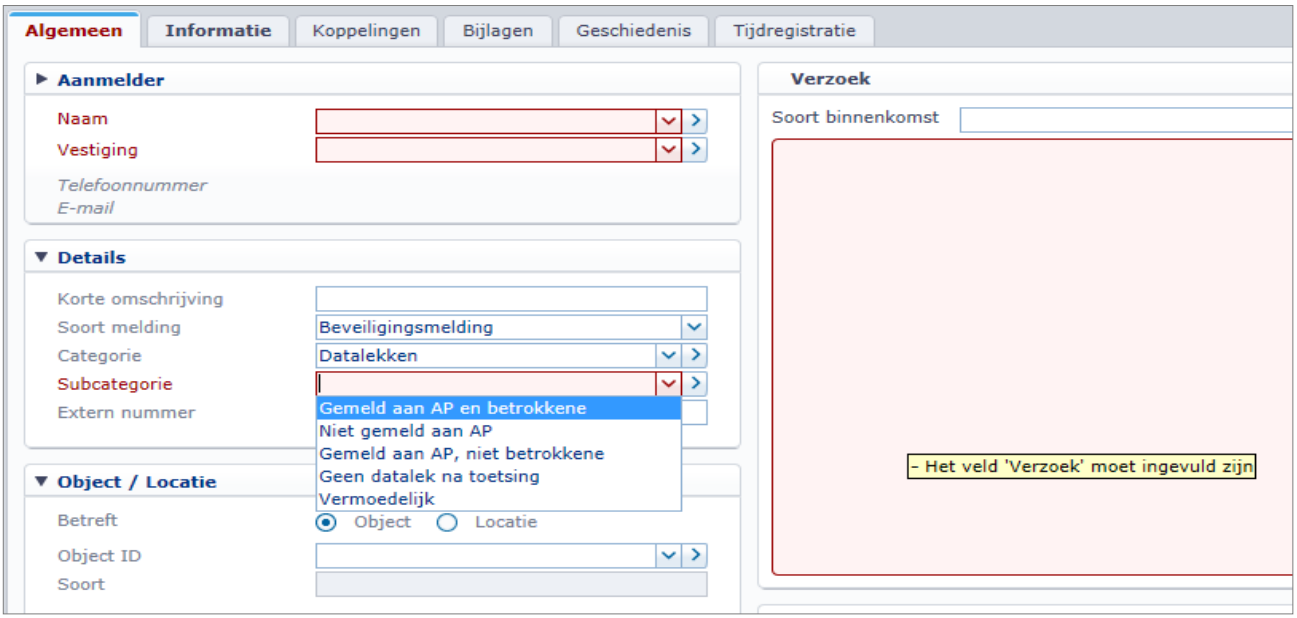
Wanneer bij een datalek persoonsgegevens onbedoeld aan een derde zijn verstrekt, dan verzoekt de Nationale ombudsman de ontvanger om deze gegevens retour te zenden of te vernietigen. De No tracht

hiermee de negatieve gevolgen van het datalek te beperken.

De FG draagt zorg voor het verzoek aan de onterechte ontvanger(s). In het verzoek wordt expliciet aangegeven welke stukken de ontvanger moet vernietigen of retourneren. Bij een groot aantal stukken kunnen deze ook groepsgewijs worden aangeduid (bijvoorbeeld “Een dossier met correspondentie afkomstig van Instantie X”). Indien de onterechte ontvanger niet binnen twee weken reageert, wordt een herinnering verzonden. Als ook hier niet op wordt gereageerd, wordt door de FG op basis van de aard en omvang van het datalek bepaalt of en welke vervolgactie past.

Afhankelijk van de beslissing van de FG, wijzigt hij/zij de subcategorie van het datalek in Topdesk in:

- Geen datalek na toetsing
- Niet gemeld aan AP
- Gemeld aan AP, niet aan betrokkene
- Gemeld aan AP en betrokken



Deze subcategorie dient als basis voor rapportages. De meldingen in de categorie “Gemeld aan AP, niet aan betrokkene” dienen drie jaar na afhandeling, minimaal jaarlijks opnieuw beoordeeld te worden door de FG (zie “Jaarlijkse opvolging”).

5. Eerste melding op basis van onvolledige informatie

De AVG geeft als richtlijn dat meldingen van datalekken binnen 72 uur moeten plaatsvinden. In artikel 33 lid 4 AVG wordt vermeld dat indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken de informatie (zonder vertraging) in stappen verstrekt kan worden. Mocht het niet mogelijk zijn om alle informatie op het ‘formulier melding datalek’ in te vullen binnen 24 uur na de eerste registratie van het datalek, dan wordt het formulier incompleet toegevoegd aan de melding. De FG verzorgt een eerste melding bij de Autoriteit Persoonsgegevens en indien nodig aan de betrokkene(n). De FG volgt hierbij het proces voor een volledige melding. Zodra de ontbrekende informatie bekend is, verzorgt de FG een vervolgmelding aan alle partijen. In overleg met de FG kunnen deze termijnen per geval worden aangepast.

7. Eisen aan derde partijen in de verwerkersovereenkomst

Wanneer derden namens de Nationale ombudsman persoonsgegevens verwerken, moeten een verwerkersovereenkomst zijn opgesteld. In deze overeenkomst worden naast de reguliere zaken onder andere ook de volgende punten uitgewerkt:

- De verwerker draagt zorg voor structurele en beheerste maatregelen waarmee persoonsgegevens van de No adequaat worden beschermd tegen datalekken, waarmee een datalek snel kan worden geconstateerd en waarmee de impact van een datalek zo klein als mogelijk kan worden gehouden. De verwerker toont aan dat zijn informatiebeveiliging adequaat is in een jaarlijks overleg met de No, bijvoorbeeld door overleggen van een ISO 27001 certificaat.
- De verwerker heeft de eindverantwoordelijkheid voor de beveiliging van (persoons)gegevens van de No toegewezen aan een medewerker die als contactpersoon voor de No optreedt;
- De verwerker heeft de verplichting om (vermoedelijke) datalekken zo snel als mogelijk, binnen de vastgestelde termijn (bijvoorbeeld 24 uur (klokuren: inclusief avonduren, het weekend en feestdagen)), aan de FG van de No te melden. De verwerker vult samen met de FG het formulier datalekken in en geeft aanvullende informatie waar dit volgens de No nuttig is
- De verwerker zal zich maximaal inspannen om het datalek te beperken, de impact van een datalek zo klein mogelijk te maken;

- De No heeft het recht om de staat van informatiebeveiliging van de verwerker periodiek of naar aanleiding van een incident te (laten) controleren (eventueel via een formele audit). De bewerker zal hieraan maximale medewerking verlenen.

8. Bewaartermijnen

De wet schrijft niet voor hoe lang het overzicht van datalekken moet worden bewaard. De No hanteert een minimale bewaartermijn van minimaal1 jaar.

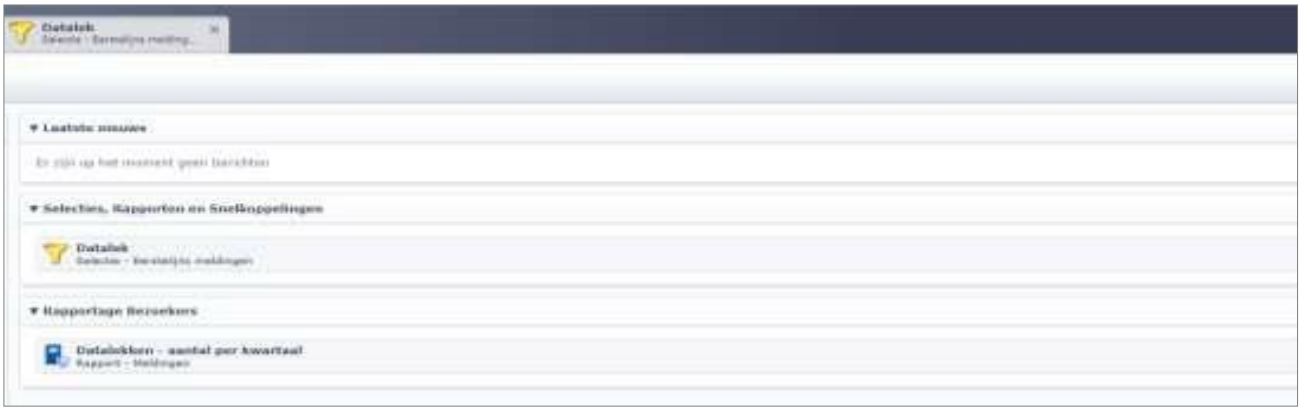
In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren. Indien melding aan de betrokkene(n) achterwege blijft, dan geldt een minimale bewaartermijn van 3 jaar. Hierdoor is het mogelijk op een later moment de betrokkene(n) bij een datalek alsnog te informeren, bijvoorbeeld omdat de maatregelen die de gelekte persoonsgegevens moeten beschermen tegen misbruik, door voortschrijdende techniek kunnen worden doorbroken. Slechts indien is vastgesteld dat het datalek geen ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene en er geen zwaarwegende redenen zijn geweest, geldt een bewaartermijn van minimaal een jaar.

9. Jaarlijkse opvolging van datalekken die niet aan betrokkene zijn gemeld

Indien melding aan de betrokkene(n) achterwege blijft, dan controleert de FG minimaal jaarlijks gedurende drie jaar of het datalek alsnog moet worden gemeld. De FG controleert hierbij of het datalek op basis van nieuwe ontwikkelingen en inzichten, alsnog invloed op de persoonlijke levenssfeer van de betrokkene kan hebben. Zo kan een datalek waarbij gegevens in versleutelde vorm zijn gestolen in eerste instantie niet worden gemeld omdat de gegevens niet te ontsleutelen zijn door derden. Als later blijkt dat een kwetsbaarheid in het algoritme voor versleuteling is gevonden, dan kunnen de gegevens hiermee (mogelijk) worden ontsleuteld en meldt de FG het datalek aan de betrokkene.

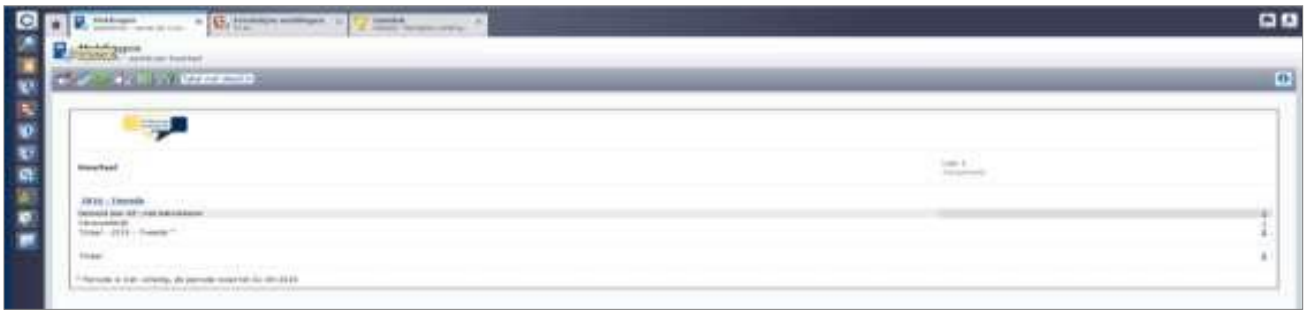
10. Rapportages in Topdesk

In Topdesk is een filter en een rapportage “Datalek” beschikbaar voor de FG en security officer, waarmee alle datalekken kunnen worden bekeken:



Onderstaande afbeelding bevat voorbeelduitvoer van het filter:

Daarnaast is een standaardrapportage op basis van bovenstaand filter opgenomen. Dit overzicht bevat op het hoogste niveau aantallen per (sub)categorie waarop kan worden doorgeklikt:



Bovenstaande rapportages kunnen worden gebruikt voor periodieke rapportages aan het management team en voor de jaarlijkse controle van datalekken door de FG die niet aan betrokkenen zijn gemeld.

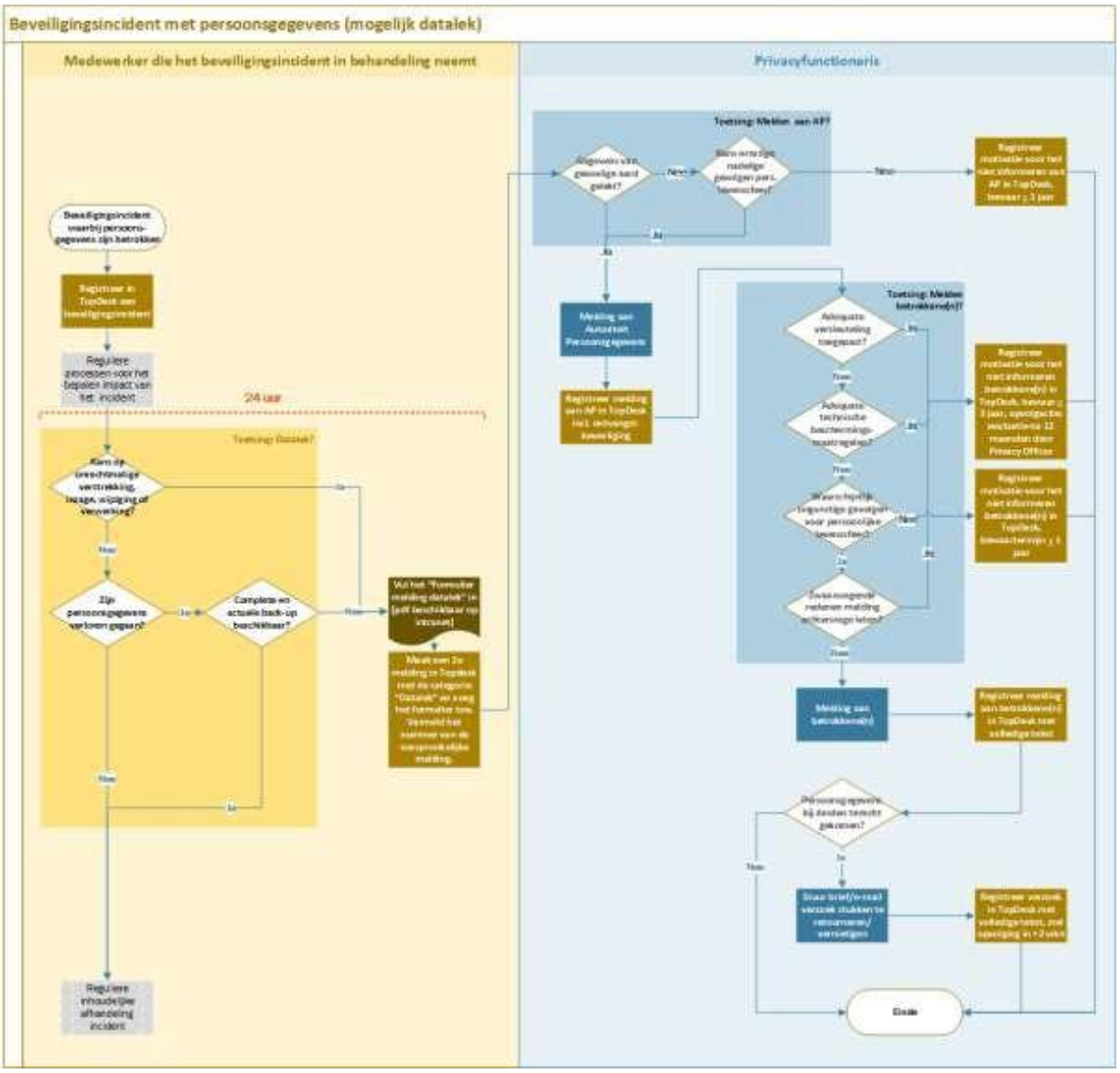
11. Controle op naleving

Vanuit het principe van functiescheiding, voert de CISO jaarlijks controles uit op de naleving van het protocol meldplicht datalekken door de medewerkers van de Nationale ombudsman.

De FG controleert jaarlijks de bepalingen in de gesloten verwerkersovereenkomst door de verwerkers van gegevens van de No. De verwerkersovereenkomsten zijn opgenomen in het verwerkingsregister.

12. Procesdiagram

Bij een beveiligingsincident waarin persoonsgegevens zijn betrokken worden de stappen uit onderstaand procesdiagram uitgevoerd.



In dit diagram zijn de volgende activiteiten niet nader uitgewerkt:

- Gedeeltelijke meldingen, waarbij nog niet alle informatie beschikbaar is en het proces van melden meerdere keren wordt doorlopen.
- Bestaande processen voor afhandeling van (beveiligings)incidenten

Bijlage 1: Melden datalekken

De belangrijkste vraag is wat de mogelijke impact is op de betrokkene(n) van het datalek. Afhankelijk van de impact moet er een melding gedaan worden aan de AP en de betrokkene(n).

Melden aan toezichthouder

Stel vast wat de mogelijke impact is op de betrokkene(n) van het datalek.

Vanuit de Europese Guidelines meldplicht datalekken worden de volgende criteria genoemd die kunnen helpen bij het vaststellen van het risico voor het individu:

- **Het type datalek:** een inbreuk waarbij medische informatie aan niet-geautoriseerde partijen is bekendgemaakt, kan andere gevolgen hebben voor een persoon dan een lek waarbij de medische gegevens van een persoon verloren zijn gegaan en niet langer beschikbaar zijn.

- **De aard, gevoeligheid en hoeveelheid van persoonlijke gegevens:** hoe gevoeliger de gegevens, hoe groter het risico op schade is voor de getroffen personen. Een kleine hoeveelheid zeer gevoelige persoonlijke gegevens kan een groot effect hebben op een persoon en een groot aantal details kan een groter scala aan informatie over die persoon onthullen. Ook kan een inbreuk op grote hoeveelheden persoonlijke gegevens van invloed zijn op een overeenkomstig groot aantal personen.

- **Eenvoud waarmee personen geïdentificeerd kunnen worden:** Identificatie kan direct of indirect mogelijk zijn uit de geschonden gegevens, maar het kan ook afhankelijk zijn van de specifieke context van de inbreuk en de openbare beschikbaarheid van gerelateerde persoonlijke gegevens

- **Ernst van de gevolgen voor het individu:** als de overtreding betrekking heeft op persoonlijke gegevens over kwetsbare personen, kunnen deze een groter risico op schade toebrengen.

- **Speciale kenmerken van het individu:** een inbreuk kan van invloed zijn op persoonlijke gegevens met betrekking tot kinderen of andere kwetsbare personen, die daardoor mogelijk een groter risico op gevaar lopen.

- **Het aantal getroffen personen:** een datalek kan slechts één of enkele individuen betreffen of enkele duizenden of nog veel meer. Over het algemeen geldt dat hoe groter het aantal getroffen personen, hoe groter de impact van een datalek kan zijn.

- **Speciale kenmerken van de verwerkingsverantwoordelijke:** de aard en de rol van de verwerkingsverantwoordelijke en zijn activiteiten kunnen van invloed zijn op het risiconiveau voor personen als gevolg van een datalek. Een medische organisatie zal bijvoorbeeld speciale categorieën persoonlijke gegevens verwerken, wat betekent dat er een grotere bedreiging is voor individuen als hun persoonlijke gegevens worden geschonden, vergeleken met een verzendlijst van een krant.

Wanneer het datalek geen risico vormt voor de betrokkene(n) dan hoeft het datalek niet gemeld te worden aan de AP. In alle overige gevallen dient het datalek – in ieder geval binnen 72 uur - gemeld te worden aan de AP (https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0).

Melden aan betrokkene(n)

Wanneer het risico op ongunstige gevolgen voor de betrokkene(n) erg hoog is, moet het datalek over het algemeen gemeld worden aan de betrokkene(n). Wanneer het risico gemiddeld of laag is kan de melding aan de betrokkene(n) vaak achterwege blijven.

Deze afweging dient per geval gemaakt te worden. Bij voorkeur wordt de afweging ondersteund door het management.

Een melding aan betrokkene(n) is niet verplicht indien:

1. passende technische en organisatorische beschermingsmaatregelen genomen en toegepast zijn op de persoonsgegevens waarop het datalek betrekking heeft. Met name die maatregelen die persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
2. de verwerkingsverantwoordelijke achteraf maatregelen heeft genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
3. de mededeling zoveel moeite kost, dat het niet meer in verhouding staat. In dat geval wordt er in plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkene(n) even doeltreffend worden geïnformeerd.

Wat in ieder geval gemeld moet worden aan de AP:

- de aard en omvang van de inbreuk in verband met persoonsgegevens, waar mogelijk met vermelding van de categorieën van betrokkenen, de persoonsgegevensregisters, en een schatting van het aantal betrokkenen in kwestie;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Wat in ieder geval gemeld moet worden aan de betrokkene(n):

- Omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk voor betrokkenen;
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Bijlage 2: Voorbeelden

Hieronder worden een aantal voorbeelden gegeven van beveiligingsincidenten waarbij persoonsgegevens zijn betrokken. Deze voorbeelden zijn illustratief, ieder (vermoedelijk) datalek moet individueel worden beoordeeld.

Document in het verkeerde dossier geplaatst en mogelijk meegestuurd

Een collega treft in een Verseon-dossier een brief aan die bij een ander dossier hoort. In de brief staat medische informatie. Het is niet duidelijk of de brief aan overheidsinstanties is meegestuurd tijdens de klachtbehandeling.

Omdat de brief bijzondere persoonsgegevens bevat en onbevoegde inzage/verspreiding door derden niet kan worden uitgesloten, is dit een datalek. De medewerker vult het 'formulier melden datalek' en stuurt dit naar de FG. De medewerker verwijdert de brief uit het dossier en slaat deze in het juiste dossier op. De FG beoordeelt het datalek en besluit dit te melden bij de Autoriteit persoonsgegevens omdat de brief gevoelige informatie bevat. Ook informeert de FG de betrokkene, omdat kennisname door derden niet redelijkerwijs kan worden uitgesloten en dit mogelijk van invloed kan zijn op de persoonlijke levenssfeer van de betrokkene.

De FG stuurt een brief naar de betrokkene om hem te informeren en te adviseren over mogelijke maatregelen om het effect hiervan te minimaliseren. Ook stuurt hij een standaard e-mail naar de ontvanger binnen de overheidsinstantie met het verzoek de brief te vernietigen of te retourneren.

Document in het verkeerde dossier geplaatst en alleen intern ingezien

Een collega treft in een Verseon-dossier een brief aan die bij een ander dossier hoort. In de brief staat informatie over de financiële situatie van een betrokkene. Bij controle blijkt dat de brief alleen door klachtbehandelaars binnen de Nationale ombudsman is ingezien.

De brief bevat gevoelige persoonsgegevens. Door het misplaatsen van de brief in een ander dossier is echter geen onrechtmatige inzage ontstaan. In de huidige werkwijze van de No hebben alle klachtbehandelaars toegang tot alle dossiers, waardoor de informatie door het misplaatsen niet door meer personen kon worden ingezien. Alle klachtbehandelaars zijn gebonden aan een ambtseed en geheimhouding. Alhoewel slordig, is hier geen sprake van een datalek.

Verkeerd geadresseerde e-mail

Tijdens het opstellen van een e-mail typt de medewerker het begin van een e-mailadres in Outlook in. Outlook geeft vervolgens een verkeerde suggestie voor de geadresseerde, die per ongeluk door de medewerker wordt gekozen. De e-mail die gevoelige informatie bevat wordt hierdoor verzonden aan de verkeerde persoon buiten de No.

Nadat de medewerker de fout constateert, registreert hij het datalek door het invullen van het 'formulier melden datalek'. De FG meldt vervolgens het datalek bij de Autoriteit Persoonsgegevens indien de persoonlijke levenssfeer van de betrokkene kan worden geraakt. Indien nodig wordt de betrokkene ook op de hoogte gesteld. De onjuiste ontvanger wordt verzocht de e-mail te verwijderen.

Retourpost

Een brief met inhoudelijke en gevoelige informatie over een klacht die aan een burger is verzonden, komt terug als “niet bezorgd”. De brief is geopend en weer dichtgeplakt met plakband. Omdat de brief persoonsgegevens bevat en de ontvanger deze heeft geopend en waarschijnlijk heeft gelezen, is er sprake van een datalek. De medewerker vult het ‘formulier melden datalek’ in en noteert de gegevens van de onjuiste ontvanger bij de TopDesk melding.

De FG meldt het datalek aan de AP indien de inhoud gevoelige gegevens bevat en zijn ingezien door derden. Ook meldt hij het datalek aan de betrokkene, omdat er een kans is dat de onjuiste ontvanger de gevoelige informatie misbruikt. Ten slotte stuurt de FG een bericht aan de ontvanger met het verzoek de inhoud van de brief vertrouwelijk te behandelen.

Diefstal of verlies van papieren dossierstukken

Een medewerker van de No neemt zaakinhoudelijke stukken in een tas mee naar huis. Tijdens het vervoer wordt de tas gestolen. De medewerker doet aangifte bij de politie. Omdat het waarschijnlijk is dat de dief de papieren met persoonsgegevens zal inzien of (onveilig) zal wegwerpen, vult de medewerker het ‘formulier melden datalek’ in en registreert hij het datalek in TopDesk. De medewerker inventariseert hierbij welke persoonsgegevens in de tas aanwezig waren en van welke burgers.

De FG meldt het datalek aan zowel het AP als de betrokkene(n) omdat niet kan worden uitgesloten dat de gegevens onrechtmatig worden verwerkt, met ongunstige effecten op hun persoonlijke levenssfeer. Indien de tas op slot was en ongeopend wordt teruggevonden, kan de FG deze melding intrekken.

Diefstal of verlies van een laptop

De laptop van een medewerker wordt gestolen. Omdat de medewerker geen documenten lokaal op de laptop opslaat, en de laptop beschermd is met een encryptieprotocol (BitLocker) is hier geen sprake is van een datalek. Deze motivatie wordt in TopDesk vastgelegd.

Diefstal of verlies van een laptop

De laptop van een medewerker wordt gestolen. Op deze laptop zijn dossierstukken opgeslagen waarin persoonsgegevens zijn opgenomen. Omdat de laptop is versleuteld met een standaard encryptieprotocol (BitLocker), is het voor derden redelijkerwijs niet mogelijk om toegang te krijgen tot de opgeslagen persoonsgegevens en is er geen sprake van een datalek. De melding aan de AP en betrokkene(n) kan daarom achterwege blijven. Indien door voortschrijdende techniek blijkt dat later ontsleuteling mogelijk is geworden, verzorgt de FG alsnog een melding aan de AP en de betrokkene(n). Hij gebruikt hierbij de informatie zoals in TopDesk is opgeslagen.

ICT-calamiteit waarbij een database verloren gaat

Door een menselijke fout raakt een database met persoonsgegevens corrupt, waardoor deze onleesbaar of verminkt worden. Door de aanwezige back-up en herstelprocedures is het mogelijk een kopie van de gegevens terug te zetten. Hierdoor is er geen sprake van een datalek. Dit wordt vastgelegd in TopDesk.

Phishing waarbij inloggevens zijn gestolen

Een medewerker heeft een factuur in Pdf-formaat geopend waarin malware was verstopt. De malware onderschepte vervolgens inloggegevens van de medewerker, waarmee extern toegang kan worden verkregen

tot een netwerkschijf met vertrouwelijke persoonsgegevens.

De medewerker meldt het beveiligingsincident via TopDesk, het gebruikersaccount wordt geblokkeerd en de ICT-afdeling verwijdert de malware. Het incident wordt aangemerkt als datalek omdat niet kan worden uitgesloten dat derden toegang hebben gekregen tot persoonsgegevens. Het onderzoek van de logbestanden waarmee kan worden uitgesloten dat derden daadwerkelijk toegang hebben gekregen tot persoonsgegevens loopt nog.

Na 24 uur wordt in overleg met de FG besloten langer te wachten op de resultaten van het onderzoek. Na 2,5 dagen (60 uur) is het onderzoek nog in volle gang en doet de FG een eerste melding bij de Autoriteit Persoonsgegevens, waarbij hij aangeeft dat de aard en omvang van het datalek nog in onderzoek zijn. Na 96 uur blijkt dat de inloggegevens niet zijn gebruikt bij inlogpogingen door derden. De FG meldt het incident af bij het AP.

nationale ombudsman

Formulier melding datalek

Dit formulier is bedoeld om een melding te maken van een (mogelijk) datalek. De wet meldplicht datalekken verplicht de Nationale ombudsman om datalekken binnen de organisatie te registreren en te melden. Een datalek is een incident waarbij persoonsgegevens, waarvoor wij verantwoordelijk zijn, zijn gelekt naar personen of instanties die geen toegang mogen hebben tot deze gegevens.

Melding
Meldt het datalek binnen 24 uur via dit formulier en stuur het per e-mail naar de interne mailbox:
[redacted] nationaleombudsman.nl

Let op! Stuur geen overige correspondentie of stukken mee met dit formulier. Informeer ook je manager over het datalek en deze melding.

Melder

1a. Naam:	
1b. Afdeling:	

Over het incident

2a. Op welke datum vond het incident plaats?	Op ☐ Tussen ☐ en ☐ ☐ Nog niet bekend
2b. Welke ongeoorloofde actie heeft plaatsgevonden?	☐ Lezen/inzien ☐ Veranderen ☐ Diefstal ☐ Kopiëren ☐ Vernietiging ☐ Nog niet bekend
2c. Welk type gegevens-drager(s) zijn betrokken?	☐ Laptop ☐ Tablet ☐ Smartphone ☐ E-mail ☐ Brief ☐ Fax ☐ Verseon ☐ Netwerkschijf ☐ Papieren stuk ☐ Website ☐ Social media: ☐ ☐ Overige: ☐
2d. Wat is de oorzaak?	☐ Diefstal van gegevensdragers ☐ Verkeerd geadresseerd ☐ Verlies van gegevensdragers ☐ Teveel geadresseerden ☐ Onveilig vernietigen/wegwerpen ☐ Verkeerd bezorgd ☐ Scherm niet vergrendeld ☐ Niet aangekomen ☐ Onbeheerd achterlaten stukken ☐ Verkeerde autorisaties ☐ Indringer in het pand ☐ Dataverlies zonder back-up ☐ Teveel gegevens ingeleverd ☐ Digitale inbraak, hacking ☐ Verkeerde gegevens geleverd ☐ Phishing (e-mail, telefonisch

	☐ Overige:
2e. Korte beschrijving van het incident:	

Over de gegevens

3a. Om welk type persoons-gegevens gaat het?	☐ Naam, adres- en woonplaatsgegevens ☐ Telefoonnummers ☐ E-mail adressen of gebruikersnamen op social media ☐ Toegangsgegevens (bijv. inlognaam/wachtwoord ☐ Financiële gegevens (bijv. rekeningnummer) ☐ Dossiernummer ☐ Burgerservicenummer (BSN) of SoFi-nummer ☐ Kopieën van legitimatiebewijzen (bijv. paspoort, rijbewijs ☐ Geslacht, geboortedatum en/of leeftijd ☐ Bijzondere persoonsgegevens (bijv. ras, etniciteit, religie, politieke overtuiging, vakbondslidmaatschap, criminele gegevens, seksuele leven, medische gegevens) ☐ Overige
3b. Van hoeveel personen zijn persoonsgegevens betrokken bij het incident?	Minimaal: Maximaal:
3c. Bevat de groep mensen van wie de gegevens zijn gelekt:	☐ Minderjarigen ☐ Personen in andere EU-landen ☐ Overige kwestbare groepen
3d. Omschrijf de groep mensen van wie de gegevens zijn gelekt:	
3e. Welke gevolgen kan het datalek hebben voor de persoonlijke levenssfeer van de betrokkenen?	☐ Stigmatisering of uitsluiting ☐ Schade aan de gezondheid ☐ Blootstelling aan (identiteit)fraude ☐ Blootstelling aan spam of phishing ☐ Overige:
3f. Waren de gegevens versleuteld, gehast of op andere wijze onbegrijpelijk of ontoegankelijk gemaakt?	☐ Nee ☐ Ja, op de volgende wijze: ☐ Deel, op de volgende wijze: