nationale ombudsman

Retouradres: Postbus 93122, 2509 AC Den Haag

[redacted]

Geachte [redacted],

Datum
19 februari 2026

Onderwerp
Woo-besluit datalekken

Ons nummer
2368935

Uw kenmerk

Bijlage(n)

Contactpersoon
[redacted]

Op 26 november 2025 heeft u een verzoek om informatie ingediend waarbij u een beroep doet op de Wet open overheid (Woo).
U vraagt om:

1. Documenten van de totstandkoming van het overzicht dat bij Woo-besluit van 17 augustus 2023 openbaar is gemaakt.
2. Documenten die anderszins betrekking hebben op een of meerdere van de datalekken die zich in 2022 hebben voorgedaan.
3. Documenten openbaar te maken waarin tot uitdrukking komt welke datalekken zich na 2022 nog hebben voorgedaan, wat de Nationale ombudsman naar aanleiding van die datalekken heeft ondernomen, welke maatregelen sinds 2022 zijn genomen ter voorkoming van datalekken en wat is gedaan ter vergroting van het AVG-bewustzijn binnen de organisatie.

Uw verzoek wordt aangemerkt als verzoek om openbaarmaking op grond van artikel 4.1 van de Wet open overheid (Woo).

Ik besluit uw verzoek deels in te willigen en deels af te wijzen
Op basis van uw verzoek is gezocht naar de informatie over datalekken in de door u aangegeven periode in ons zaaksysteem, de netwerkschijven en mailboxen van betrokken medewerkers.
Er zijn elf documenten gevonden waarvan één document is gegenereerd. Deze documenten zijn benoemd in de inventarislijst.

Hieronder ga ik, per onderdeel, in op uw verzoek.
Verzoek 1.
Er zijn geen documenten over de totstandkoming van het overzicht dat bij Woo-besluit van 17 augustus 2023 openbaar is gemaakt. De totstandkoming betreft een handeling (genereren van een overzicht uit het registratiesysteem). Derhalve zijn er geen documenten.

Verzoek 2.
Dit onderdeel valt buiten de reikwijdte van het verzoek. Het verzoek om alle documenten die betrekking hebben op de datalekken die zich in 2022 hebben voorgedaan, is al beantwoord tijdens de behandeling van het door u ingediende bezwaarschrift tegen het Woo-besluit van 17 augustus 2023.
Ik haal hier de reactie uit deze beslissing op bezwaar nogmaals aan:

> "Bij het primaire besluit van 17 augustus 2023 is een overzicht openbaar gemaakt waarin alle datalekken in 2022 zijn opgenomen. In uw bezwaarschrift geeft u aan dat de onderliggende documenten die geleid

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

hebben tot de informatie die in dit overzicht is opgenomen, eveneens vallen onder uw verzoek, daar u stelt ook te hebben gevraagd om alle documenten.
Ik ga er vanuit dat u hiermee doelt op de datalekken zelf.

Een datalek zelf is echter geen document in de zin van de Woo. De AVG definieert een datalek in artikel 4, twaalfde lid (als 'inbreuk in verband met persoonsgegevens') als volgt: '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'.
Uit deze definitie vloeit voort dat een datalek een feitelijke handeling is, die leidt tot een inbreuk in de zin van voornoemde bepaling. Een datalek is dus zelf geen document in de zin van de Woo en kan dan ook niet worden verstrekt of openbaar gemaakt."

Verzoek 3.
Ten aanzien van het verzoek om documenten waarin tot uitdrukking komt welke datalekken zich na 2022 hebben voorgedaan en wat is ondernomen door de Nationale ombudsman ten aanzien van het vergroten van het AVG-bewustzijn zijn, zoals hiervoor gemeld, elf documenten aangetroffen.
Deze documenten zijn benoemd in de inventarislijst en toegevoegd bij dit besluit.

Waarom in sommige documenten informatie niet leesbaar is
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 per document aangegeven welke uitzonderingsgronden van toepassing zijn geweest bij het weglakken.

Het overzicht van datalekken na 2022 (document 1) maak ik in zijn geheel openbaar.
Voor wat betreft het vergroten van het AVG-bewustzijn, verwijs ik u onder andere naar de al openbare informatie op onze website. U treft hieronder de links aan.
Informatie over AVG-compliance bij de Nationale ombudsman | Nationale ombudsman
Informatie over de Privacy Officer | Nationale ombudsman

Informatie die met de aanduiding 'J' onleesbaar is gemaakt
Op grond van artikel 5.1, tweede lid, aanhef en onder e, van de Woo, kan ik geen informatie openbaar maken als dit de persoonlijke levenssfeer schaadt en dit belang zwaarder weegt dan het algemeen belang van openbaarmaking. 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 betrokkenen niet bekend wordt omdat dit hun privacy kan schaden. Dat vind ik niet wenselijk. Daarom maak ik deze persoonsgegevens niet openbaar.

Informatie die met de aanduiding 'N' onleesbaar is gemaakt
Op grond van artikel 5.1 lid 2 sub i maak ik die informatie niet openbaar omdat dit het goed functioneren van de organisatie kan schaden.

Ik ben van mening dat openbaarmaking van de informatie in deze documenten niet het algemeen belang dient. Openbaarmaking van de documenten kan schadelijke gevolgen hebben voor de bescherming van persoonsgegevens binnen en het functioneren van de organisatie. Dat vind ik niet wenselijk.
Met de gegeven informatie is overigens wel inzichtelijk gemaakt dat de organisatie stappen onderneemt ten aanzien van het vergroten het AVG-bewustzijn en het beperken van datalekken door middel van campagnes.

Informatie die met de aanduiding 'T' onleesbaar is gemaakt
In een aantal documenten is informatie onleesbaar gemaakt met de aanduiding 'T'. Deze informatie betreft de informatie over onze interne webpagina en heeft geen betrekking op het onderwerp van uw verzoek. Deze informatie valt buiten de reikwijdte van uw verzoek en wordt daarom niet openbaar gemaakt.

Wijze van bekendmaking
Naast dat het besluit aan u wordt toegezonden, zal het (geanonimiseerde) besluit met 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 [redacted]. Mailen naar woo@nationaleombudsman.nl kan ook. Denk er dan aan om uw dossiernummer (2368935) te vermelden.

Met vriendelijke groet,
namens de Nationale ombudsman,

[redacted]

Hanneke van Essen
Algemeen directeur

nationale ombudsman

Ons nummer
2368935

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 2368935

		Woo artikel
1	Overzicht datalekken 2023-2025	-
2	Interne berichtgeving toename datalekken (27-12-2023)	5.1-2e, 5.1-2i, buiten reikwijdte
3	Interne aankondiging campagne Veilig en bewust werken (12-9-2024)	5.1-2e, buiten reikwijdte
4	Intern bericht opleiding AVG-vertegenwoordigers (15 oktober 2024)	Buiten reikwijdte
5	Intern berichtgeving nieuwe maatregel postverzending - aangetekend versturen (10 juni 2025)	5.1-2e, buiten reikwijdte
6	Interne berichtgeving webinars (30-09-2025)	5.1-2e, buiten reikwijdte
7	Aankondiging webinars Algemeen directeur (12-10-2025)	5.1-2e, buiten reikwijdte
8	AVG onboardingsessie	5.1-2i
9	Rapportages fase 1 en Plan van Aanpak fase 2 (maart 2024)	5.1-2e, 5.1-2i
10	Rapportage fase 2 en Plan van Aanpak fase 3 (augustus 2025)	5.1-2e, 5.1-2i, buiten reikwijdte
11	Voorstel webinars Security awareness fase 3	-

Datalekken van 2023 tot en met november 2025

Datum melding	gemeld aan AP?	Aard datalek	Maatregelen
01/27/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
02/02/2023	Niet gemeld aan AP	laptop gestolen	Laptop Remote gewiped.
03/01/2023	Niet gemeld aan AP	brief naar verkeerd adres	adres aangepast in Zaaksysteem. Onrechtmatige ontvanger verzocht brief te retourneren of vernietigen
03/02/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
03/02/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	geen verdere actie
03/07/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
03/14/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
03/15/2023	Niet gemeld aan AP	ontvangstbevestiging naar verkeerde ontvanger	contactgegevens aangepast in zaaksysteem. Onrechtmatige ontvanger verzocht bericht te vernietigen.
03/23/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
03/30/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
04/03/2023	Niet gemeld aan AP	Brief naar verkeerd (oud) adres	gegevens aangepast in Zaakysteem. Onrechtmatige ontvanger heeft aangegeven brief te vernietigen
05/11/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
05/24/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
06/13/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen.
06/13/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
06/13/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
06/20/2023	Niet gemeld aan AP	intern Datalek, onterechte ontvangers bijlage emailbericht	Afzender uitgelegd dat informatie alleen verstuurd moet worden naar personen die daar recht op hebben.
06/27/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
07/11/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
07/24/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
08/02/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
08/03/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
08/08/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
08/29/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	geen verdere actie
10/26/2023	Gemeld aan AP, niet betrokkene	beveiligingsincident p-direkt	Melding vanuit het Rijk, niet door ons veroorzaakt. Fout in P-direkt kan mogelijk leiden tot een datalek. Geregistreerd om opvolging en afhandeling te monitoren. O&P Rijk heeft melding gedaan bij de AP.
10/31/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
12/06/2023	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
12/19/2023	Niet gemeld aan AP	eindbrief naar verkeerd adres	Onrechtmatige ontvanger verzocht bericht te vernietigen. Verzoeker is op de hoogte gesteld
01/15/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.

02/05/2024	Niet gemeld aan AP	emailadressen verzoekers in CC ipv BCC	Gewezen op gebruik CC vs BCC. geen verdere actie.
02/05/2024	Niet gemeld aan AP	Brief vz naar oude adres	verzoeker correspondeerde met oud adres. Nieuw adres nu aangepast in Zaaksysteem. Brief retour ontvangen
02/21/2024	Niet gemeld aan AP	Openingsbrief naar oude adres vz	oud adres in systeem aangepast. Verkeerde ontvanger heeft brief retour gestuurd.
02/26/2024	Niet gemeld aan AP	Vetragingsbericht mailadres vz ingezien	Gewezen op gebruik CC vs BCC. geen verdere actie.
04/02/2024	Niet gemeld aan AP	Medewerker gegevens zichtbaar bij uitbellen	Probleem bij Odido. Is in de loop van de week opgelost
04/09/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
04/15/2024	Geen datalek na toetsing	brief naar verkeerde huisnummer	Brief ongeopend retour ontvangen. Behandelaar gewezen op hoe NAW gegevens uit zaaksysteem kunnen worden overgenomen ipv over te typen.
04/16/2024	Niet gemeld aan AP	email beantwoord ipv doorsturen	geen verdere actie
04/17/2024	Geen datalek na toetsing	email naar verkeerde mailadres	e-mailbericht is niet afgeleverd. Niet bestaand adres.
04/25/2024	Geen datalek na toetsing	rapport brief naar oude adres advocaat	Brief naar oud adres. Adres is aangepast in zaaksysteem. Rechtmatige Ontvanger heeft aangegeven brief alsnog ongeopend ontvangen te hebben.
05/13/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
05/28/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
05/28/2024	Niet gemeld aan AP	openingsbrief naar oud adres vz	brief naar oud adres. Adres is aangepast in zaaksysteem. Ontvanger verzocht om brief te retourneren of vernietigen.
06/13/2024	Geen datalek na toetsing	e-mails naar verkeerde ontvanger	e-mailbericht is niet afgeleverd. Niet bestaand adres.
06/19/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
06/25/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
06/26/2024	Geen datalek na toetsing	brief naar verkeerd huisnummer	brief is ongeopend retour gekomen. Adres aangepast in zaaksysteem.
07/10/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
07/12/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
07/17/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
07/31/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
08/07/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
08/20/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
08/22/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
08/27/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
09/04/2024	Niet gemeld aan AP	Datalek brief naar oud adres	oude adresgegevens in zaaksysteem verwijderd. Brief is retour gekomen.
09/10/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
09/17/2024	Niet gemeld aan AP	brief naar oude adres	Ggevens in Djuma aangepast.
09/30/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
11/27/2024	Niet gemeld aan AP	laptop tas kwijt	laptoptas is enkele uren kwijtgeweest. Zaten wel notities in, maar onduidelijk of die ingezien zijn.
12/04/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
12/11/2024	Niet gemeld aan AP	brief gevonden op kantoor	Eigenaar brief aangesproken op het laten rondslingeren van persoonsgegevens. Brief is vernietigd door melder datalek.
12/11/2024	Niet gemeld aan AP	Naam verzoeker in gepubliceerd rapport	publicatie is aangepast. Behandelaar is geinformeerd zo ook het Service Team wat de publicaties opmaakt.

12/16/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
12/19/2024	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
01/13/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
02/03/2025	Niet gemeld aan AP	phishing mail gaat rond in organisatie	medewekers gevraagd alert te zijn op phising mail en geen contactgegevens achter te laten.
02/17/2025	Niet gemeld aan AP	inloggegevens bij phishing actie, door klikken op popup zijn inloggegevens van een medewerker ontfutseld	ICT heeft vastgesteld dat er geen onterechte toegang tot systemen heeft plaatsgevonden. Inloggegevens medewerker zijn direct gewijzigd. Systeem van medewerker is korte tijd geisoleerd geweet voor onderzoek door ICT. Systeem opnieuw ingespoeld.
02/17/2025	Geen datalek na toetsing	brief naar oude adres	Brief ongeopend retour ontvangen. Rechtmatige ontvanger op de hoogte gesteld en excuus aangeboden. Adresgegeves aangepast in zaaksysteem
02/20/2025	Geen datalek na toetsing	Telefoon kwijtgeraakt	Telefoon is op afstand succesvol geblokkeerd door ICT
02/24/2025	Niet gemeld aan AP	Leverancier website heeft onversleutelde export productiedatabase van internet tijdelijk op amerikaanse database staa	Gemeld door leverancier zelf. In overleg de zaak besproken en waarom dit überhaupt is gebeurd. Export is direct verwijderd. Nieuwe afspraken gemaakt met leverancier omtrent het werken met exports.
02/24/2025	Niet gemeld aan AP	datalek verkeerde dossiernummer	verzoeker is op de hoogte gebracht en heeft correct nummer gekregen.
03/05/2025	Niet gemeld aan AP	datalek interne mail	interne mail is met teveel collega's gedeeld. Casus is in AVG-overleg besproken en dit wordt in teams verder onder de aandacht gebracht.
03/10/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
03/12/2025	Niet gemeld aan AP	brief naar verkeerde adres	Onrechtmatige ontvanger verzocht bericht te vernietigen. Gegevens in het zaaksysteem zijn aangepast.
03/24/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
03/27/2025	Gemeld aan AP en betrokkene	brief niet ontvangen door verzoeker. Bevatte gevoelige persoonsgegevens.	Mogelijk verloren gegaan bij postnl bezorging. Adres was correct. Melding gedaan bij de AP
03/27/2025	Niet gemeld aan AP	brief met ontvangstbevestiging niet ontvangen door verzoeker	Mogelijk verloren gegaan bij postnl bezorging. Brief is opnieuw verstuurd.
04/01/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
04/09/2025	Geen datalek na toetsing	mail naar verkeerde mailadres	Bij toetsing blijkt e-mailbericht niet te zijn afgeleverd. Niet bestaand e-mailadres. E-mailadres stond verkeerd in zaaksysteem. Dit is aangepast.
04/16/2025	Niet gemeld aan AP	metadata gepubliceerde documenten. Rapporten op de website kunnen namen van medewerkers bevatten in de meta	Effort is te groot om alle rapporten na te lopen. Steekproef toont aan dat niet in alle rapporten metadata zijn ingevuld. Nieuwe werkwijze is om voor publicatie de metadata na te lopen en persoonsgegevens te verwijderen waar nodig.
05/12/2025	Geen datalek na toetsing	Vertragingsbericht in dossiers met emailadressen in BCC	vertragingsberichten zijn verwijderd uit de betrokken dossiers. Klachtbehandelaars hebben voor hun werk toegang in het zaaksysteem tot gegevens van verzoekers. Geen sprake van onterechte toegang.
06/04/2025	Niet gemeld aan AP	vertragingsbericht emailadressen in CC ipv BCC	E-mailbericht is ingetrokken. Werkwijze van verzenden vertragingsberichten is aangepast zodat een dergelijke situatie niet meer kan ontstaan in de toekomst.
07/07/2025	Gemeld aan AP en betrokkene	verkeerd geadresseerde brief, brief bevat strafrechtelijke gegevens	In communicatie met verzoeker onduidelijk of brief wel of niet geopend was bij ontvangst. Voor de zekerheid melding gedaan bij de AP.
07/21/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
07/21/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
08/01/2025	Niet gemeld aan AP	verkeerde verzoeker gebeld over een zaak, door verkeerd handelen medewerker verkeerde contactpersoon gebeld.	Advies gegeven om niet gebruik te maken van contactgegevens uit documenten.
08/19/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Melding gedaan bij Leverancier vanwege fout in Zaaksysteem. Service team op de hoogte gesteld van fout in systeem en tijdelijke workaround. Onrechtmatige ontvanger verzocht bericht te vernietigen.
08/19/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Melding gedaan bij Leverancier vanwege fout in Zaaksysteem. Service team op de hoogte gesteld van fout in systeem en tijdelijke workaround. Onrechtmatige ontvanger verzocht bericht te vernietigen.

08/19/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Melding gedaan bij Leverancier vanwege fout in Zaaksysteem. Service team op de hoogte gesteld van fout in systeem en tijdelijke workaround. Onrechtmatige ontvanger verzocht bericht te vernietigen.
08/26/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
10/09/2025	Geen datalek na toetsing	brief naar verkeerd (oud) adres verzonden. Brief ongeopend retour ontvangen	geen verdere actie
11/07/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
11/13/2025	Niet gemeld aan AP	verkeerde ontvanger emailbericht	Onrechtmatige ontvanger verzocht bericht te vernietigen. Medewerker gewezen op gebruik autocomplete functie outlook en op letten bij selecteren juiste e-mailadres.
11/18/2025	Geen datalek na toetsing	verkeerd dossiernummer vermeld in onderwerpregel van mail	geen verdere actie

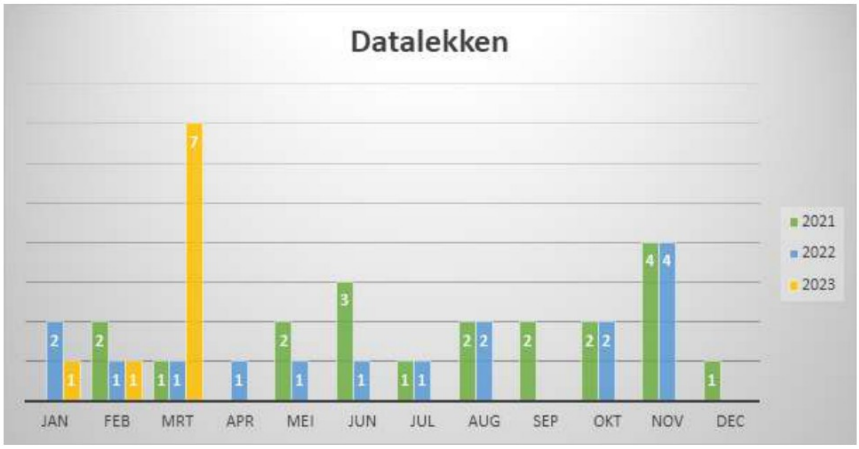
Toename in datalekken

27 maart 2023 - Laatste wijziging op 27 december 2023

Er is een flinke toename van het aantal datalekken. In dit artikel lees je hoe een datalek kan voorkomen en hoe je een datalek meldt.

Bij een datalek gaat het om vernietiging, verlies of delen van persoonsgegevens zonder dat dat de bedoeling was. Voor de hand liggende voorbeelden zijn een e-mailbericht met persoonsgegevens wat naar een verkeerde ontvanger is gegaan, een poststuk wat naar een oud adres is verstuurd, of een verloren document of usb-stick.

In de grafiek hieronder zie je vanaf 2021 hoeveel datalekken we per maand hebben geregistreerd.



In de grafiek is goed te zien dat het aantal datalekken de afgelopen jaren redelijk laag is gebleven met een gemiddelde van 2 per maand. Helaas is er deze maand sprake van een behoorlijke toename. We hebben al 7 datalekken geconstateerd en maart is nog niet voorbij.

Bij navraag blijkt het in bijna alle gevallen te gaan om e-mails met persoonsgegevens die naar een verkeerde ontvanger zijn verstuurd. Een dergelijke datalek ontstaat snel omdat we in Outlook gebruik maken van auto complete. Deze functie zorgt er voor dat e-mailadressen

automatisch worden aangevuld tijdens het typen. Handig! Maar zoals de grafiek laat zien ook niet zonder risico.

Het is belangrijk om het aangevulde adres goed te controleren voordat op 'verzenden' wordt geklikt. Blijf alert!

Registratieplicht en meldplicht

Het is goed denkbaar dat er bij ons meer datalekken plaatsvinden dan deze grafiek toont. Dit zijn immers alleen de gevallen die gemeld zijn. De AVG verplicht ons om alle datalekken op te nemen in een register. We moeten kunnen aantonen welke maatregelen we nemen om de mogelijke gevolgen van een lek te mitigeren en hoe we het in de toekomst kunnen voorkomen. In enkele gevallen geldt een meldplicht bij de Autoriteit Persoonsgegevens en bij de betrokkenen zelf. Het gaat dan met name om datalekken waarbij aannemelijk is dat de betrokkenen een groot risico lopen. Het is belangrijk dat een (vermoedelijk) datalek direct gemeld wordt zodat we snel maatregelen kunnen nemen.

Hoe meld je een datalek?

Vermoed je een datalek? Meld dat dan bij je AVG-vertegenwoordiger in je team, mail naar [redacted] of meld het lek via de knop 'Meld datalek' rechts bovenin op NoHow

datalek

Start nieuwe campagne: Veilig en bewust werken

Redactie NoHow, 12 september 2024 - Laatste wijziging op 12 september 2024

We werken met veel gevoelige informatie. Het kan ons allemaal overkomen dat we een risico onvoldoende goed inschatten of een keer een fout maken. We willen veilig werken, maar hoe moet dat en welke risico's lopen we?

Hiermee gaan we aan de slag tijdens de campagne 'Veilig en bewust werken'. We vinden het belangrijk om alle medewerkers te trainen en bewust te maken hoe we veilig kunnen werken. Daarom vertalen we wetgeving naar onze dagelijkse werkzaamheden, leren we samen risico's te herkennen en incidenten op de juiste manier te melden.

Op kantoor, onderweg en thuis

Omdat cybersecurity, informatieveiligheid en privacy veel informatie omvat, hebben we het programma opgedeeld in verschillende onderwerpen. Drie thema's volgen elkaar op:
1. Op kantoor: alles over cybercriminaliteit en veilig werken binnen kantoormuren
2. Onderweg: alles over veilig mobiel werken en diefstal
3. Thuis: alles over veilig thuiswerken en veilige verbindingen

Wat gaan we doen?

Jij bent de sleutel tot veilig werken! Per thema meld je je aan voor een webinar. Met behulp van quizzen toetsen we de opgedane kennis. Daarnaast worden we uitgedaagd door phishingsimulaties en meten we of we alert zijn en niet in phishingmails trappen. We attenderen je op het geldende beleid en geven je tips en tricks om veilig te werken.

Thema 1: Veilig werken op kantoor

Het eerste thema is 'Veilig werken op kantoor'. We wanen ons vaak veilig tussen de muren van ons pand, maar ook hier lopen we security- en privacy risico's. Een 'collega' die met je meeloopt naar binnen zonder toegangspas of een onbekende die je over de gang ziet lopen, is het bezoek van iemand? Het kan een betrouwbaar persoon zijn, maar het kan net zo goed een insluiper zijn met kwade bedoelingen. Het meenemen van laptops, mobiele telefoons en papieren is zo gedaan. Net als het plaatsen van een camera, microfoon of apparatuur om het internetverkeer uit te lezen. Tijdens het thema 'Veilig en bewust werken op kantoor' ga je

hier van alles over leren. Er zal op vier verschillende momenten een webinar worden aangeboden, zodat het voor iedereen mogelijk is om deel te nemen.

Webinars

De webinars worden op de volgende momenten aangeboden

- Maandag 23 september webinar 1 I 12:00 – 13:00
- Donderdag 3 oktober webinar 2 I 15:30 – 16:30
- Woensdag 16 oktober webinar 3 I 9:30 – 10:30
- Dinsdag 29 okt webinar 4 I 12:30 – 13:30

Meld je via deze link aan voor één van de webinars. Selecteer naast de datum ook het tijdstip voordat je een reservering maakt!

Competitie

Niets is zo leuk als een spelelement als we iets nieuws moeten leren. Om deze reden hebben we tijdens de 'Veilig en bewust werken- campagne' niet één maar twéé competities!

1. Flash Quiz Competitie: aan het einde van de thema-periode wordt er een Flash Quiz naar iedereen gestuurd via email. De Flash Quiz bestaat uit een mix van vragen waarin we de materie dat tijdens het thema behandeld is doornemen. Scoor jij met jouw team de meeste punten? Dan win je iets leuks!

2. Phishing Competitie: bij elke phishingsimulatie brengen we per team in kaart welk team de minste kliks/fails heeft en welk team uitblinkt in het snel melden van de verdachte email. Presteren jij en je team het beste? Dan wacht er een beloning!

Let the games begin!

Vragen?

Heb je vragen of opmerking over de campagne, neem dan contact op met [redacted]
[redacted]@nationaleombudsman.nl

Veilig en bewust werken

Opleiding AVG-vertegenwoordigers

Redactie NoHow, 15 oktober 2024 - Laatste wijziging op 15 oktober 2024

Op 3 oktober 2024 volgden onze AVG-vertegenwoordigers de (terugkerende) cursus voor AVG-vertegenwoordigers.

Deze cursus is bedoeld om de AVG-kennis van onze vertegenwoordigers op te frissen en te verdiepen. Zij kunnen hierdoor hun rol goed uitoefenen en fungeren als een belangrijke schakel tussen hun afdeling/team/domein en de Privacy Officer en FG. Daarnaast wordt hiermee de bewustwording over de bescherming van persoonsgegevens vergroot. Omdat dit jaar meerdere nieuwe AVG-vertegenwoordigers erbij zijn gekomen, was er grote behoefte aan deze opleiding.

Interactief

De opleiding werd verzorgd door onze partner Ilionx. Het was een interactieve cursus met diverse casussen uit de praktijk, ingebracht door de vertegenwoordigers zelf. Er vonden interessante discussies plaats, bijvoorbeeld over het noteren van (gevoelige) persoonsgegevens tijdens een telefoongesprek en het delen van persoonsgegevens met andere instanties. Het bracht ook nieuwe vragen naar voren, die verder worden uitgezocht. Kortom, het was een interessante ochtend met de AVG-groep. Ik raad iedereen aan om vooral even naar dit filmpje te kijken!

Vragen?

Heb je een privacy vraag? Stel deze aan jouw AVG-vertegenwoordiger of de Privacy Officer.

AVG

Nieuwe maatregel post: digitaal of aangetekend versturen

[redacted] 10 juni 2025 - Laatste wijziging op 10 juni 2025

We merken steeds vaker dat we post versturen, maar dat deze niet goed aankomt. Als hier persoonsgegevens in staan, moet deze niet-ontvangen post als datalek worden beschouwd. Hieronder lees je welke maatregel we nemen om deze datalekken te voorkomen.

We merken steeds vaker dat we post versturen, maar dat deze niet goed aankomt. Als hier persoonsgegevens in staan, moet deze niet-ontvangen post als datalek worden beschouwd. Hieronder lees je welke maatregel we nemen om deze datalekken te voorkomen.

Onlangs zijn er een aantal datalekken geweest die waren toe te schrijven aan wel verzonden maar niet ontvangen post. Post waarin persoonsgegevens worden vermeld en die niet goed wordt ontvangen, moet op grond van de AVG als datalek worden beschouwd. Het is immers niet bekend wie de persoonsgegevens kunnen inzien.

Helaas zijn dit datalekken waar we niet direct invloed op hebben. Als ombudsman maken we ons al langer zorgen over het functioneren van Post.nl. Het bericht hierover kun je hier lezen. Het raakt ons dus ook rechtstreeks bij de verzending van onze post aan verzoekers.

Maatregel

Ondanks dat postbezorging buiten onze invloedssfeer ligt, kunnen we het risico op een datalek als gevolg van niet bezorgde post wel verkleinen. In afstemming met onze [redacted] is besloten tot de volgende beheersmaatregel:

1) Zoveel mogelijk digitaal

Daar waar het kan communiceren we al vaak via email en worden stukken digitaal verzonden. Door ambtsdragers getekende stukken worden in ieder geval per post verstuurd en als er alleen een postadres van een verzoeker bekend is.

2) Aangetekend versturen

Een manier om een datalek te voorkomen is om post aangetekend te versturen. Van deze mogelijkheid wordt soms al gebruik gemaakt, maar er zijn nog geen afspraken over wanneer dat vanuit privacy oogpunt moet. Omdat het niet proportioneel is om alles aangetekend te versturen is ervoor gekozen om post waarin sprake is van bijzondere persoonsgegevens volgens de AVG via aangetekende post te versturen. Het gaat daarbij om de volgende persoonsgegevens:

- Persoonsgegevens waaruit iemands afkomst of etniciteit blijkt.
- Persoonsgegevens waaruit iemands politieke opvattingen blijken.
- Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken.
- Persoonsgegevens waaruit het lidmaatschap van een vakbond blijkt.
- Gegevens over iemands gezondheid.
- Gegevens over iemands seksueel gedrag of seksuele gerichtheid.
- Strafrechtelijke gegevens zijn formeel geen bijzondere persoonsgegevens, maar uiteraard wel gevoelige gegevens. Ook hiervoor geldt dat post die informatie hierover bevat aangetekend dient te worden verzonden.

Het is aan de behandelend medewerker om te beoordelen welke post aangetekend dient te worden verzonden. Als daar sprake van is dan moet je dit duidelijk aangeven aan de collega's van het servicecentrum zodat zij dit kunnen verzorgen.

Vragen?

Als je een vraag hebt over dit bericht kun je deze stellen aan mij [redacted]

datalek

Webinars

Informatiebeveiliging, 22 september 2025 - Laatste wijziging op 30 september 2025

De sleutel tot veilig werken, dat zijn wij, de medewerkers. We werken met veel gevoelige informatie. Het kan ons allemaal overkomen dat we een risico onvoldoende goed inschatten of een keer een fout maken. We willen veilig werken, maar hoe moet dat en welke risico's lopen we? In drie webinars nemen we je mee in veilig en bewust werken.

Webinars Veilig en bewust werken

Omdat cybersecurity, informatieveiligheid en privacy veel informatie omvat, hebben we het opgedeeld in drie thema's.

Op kantoor, onderweg en thuis

1. Op kantoor: alles over cybercriminaliteit en veilig werken binnen kantoormuren
2. Onderweg: alles over veilig mobiel werken en diefstal
3. Thuis: alles over veilig thuiswerken en veilige verbindingen

Thema 1: Veilig werken op kantoor

We wanen ons vaak veilig tussen de muren van ons pand, maar ook hier lopen we security- en privacy risico's. Een 'collega' die met je meeloopt naar binnen zonder toegangspas of een onbekende die je over de gang ziet lopen, is het bezoek van iemand? Het kan een betrouwbaar persoon zijn, maar het kan net zo goed een insluiper zijn met kwade bedoelingen. Het meenemen van laptops, mobiele telefoons en papieren is zo gedaan. Net als het plaatsen van een camera, microfoon of apparatuur om het internetverkeer uit te lezen.

Webinar Veilig Werken op Kantoor - Anoniem.mp4

Thema 2: Veilig werken onderweg

Of je nu in de trein zit, op een flexplek werkt of even snel je e-mails checkt in een café: onderweg werken hoort er steeds vaker bij. Maar hoe zorg je ervoor dat je gegevens en apparaten ook buiten kantoor goed beschermd zijn? In deze sessie nemen we je mee in de wereld van veilig mobiel werken. We kijken naar slimme tips om je laptop en telefoon te beveiligen, hoe je veilig gebruikmaakt van openbare wifi en wat je kunt doen om diefstal of verlies te voorkomen. Zo kun je met een gerust hart overal productief én veilig blijven werken.
Webinar Veilig Werken Onderweg - Anoniem.mp4

Thema 3: Veilig thuiswerken

Je verwacht het misschien niet, maar ook bij thuiswerken zijn er risico's. Denk bijvoorbeeld aan onveilige wifi-instellingen en het weggooien van vertrouwelijke documenten. Maar ook andere aangelegenheden in de privésfeer kunnen een risico zijn, zoals het gebruik van social media. Een kwaadwillende kan slimme aanvallen opzetten die heel geloofwaardig zijn. Het is daarom belangrijk dat we alert zijn en 'rode vlaggen' kunnen herkennen
Webinar Veilig Werken Thuis - Anoniem.mp4

Heb je nog vragen?

Neem gerust contact op met onze [redacted]

De webinar links zijn geldig tot april 2026

Jij bent de sleutel tot veilig werken!

Veilig en bewust werken Webinar

Van: Hanneke van Essen
Verzonden: zondag 12 oktober 2025 18:56
Aan: .Alle medewerkers
Onderwerp: Weekbericht 10 oktober

Dag collega's,

Veilig en bewust werken
Deze maand starten we met een 'nieuw seizoen' van *Veilig en bewust werken bij de ombudsman*. Dat doen we met webinars. Op NoHow kun je binnenkort een uitgebreidere toelichting lezen. In de zomer hebben jullie een uitnodiging ontvangen om een kennisenquête in te vullen. Op basis van de uitkomsten en jullie waardevolle input heeft Informatieregie de invulling van de komende webinars afgestemd op het kennisniveau en de leerbehoeften binnen de organisatie. We richten ons nu op twee thema's, namelijk Cyberaanvallen en Werken met persoonsgegevens.

Het is belangrijk dat we zorgvuldig omgaan met persoonsgegevens van burgers en medewerkers, dat zijn we snel met elkaar eens. Cyberdreigingen worden steeds geavanceerder en gerichter en vaak lijkt iets zo echt of betrouwbaar, dat je er makkelijker instinkt dan vroeger. Voor je het weet klik je bijvoorbeeld op een phishinglink of deel je gegevens met onbevoegden.

Een datalek kan grote impact hebben op betrokkenen en op onze organisatie. Daarom vinden we het belangrijk dat we ons allemaal bewust zijn van de methoden en de gevaren en weten hoe we moeten handelen. Daardoor verkleinen we het risico op privacy- en beveiligingsincidenten. Je kunt je voor de eerste webinar inschrijven via deze link: Webinar Thema Cyberaanvallen. Omdat het zo belangrijk is dat we allemaal veilig werken en weten hoe we dat moeten doen, zijn de webinars niet vrijblijvend. Het is de bedoeling dat jullie allemaal deelnemen.

Een hele goede week!

Groet, Hanneke

nationale ombudsman

Wat betekent de AVG voor ons?

AVG onboardingsessie

Verwerking persoonsgegevens door de ombudsman

nationale ombudsman

- AVG van toepassing op persoonsgegeven”: alle informatie die direct of indirect herleidbaar is naar een natuurlijk persoon
- Wij verwerken als organisatie veel persoonsgegevens;
  - Gewone persoonsgegevens: Naam, adres, telefoonnummer, e-mailadres
  - Bijzondere persoonsgegevens: medische gegevens, ras of etnische afkomst, religieuze overtuiging
- Taak van algemeen belang, wettelijke verplichting, gerechtvaardigd belang (voor interne processen)

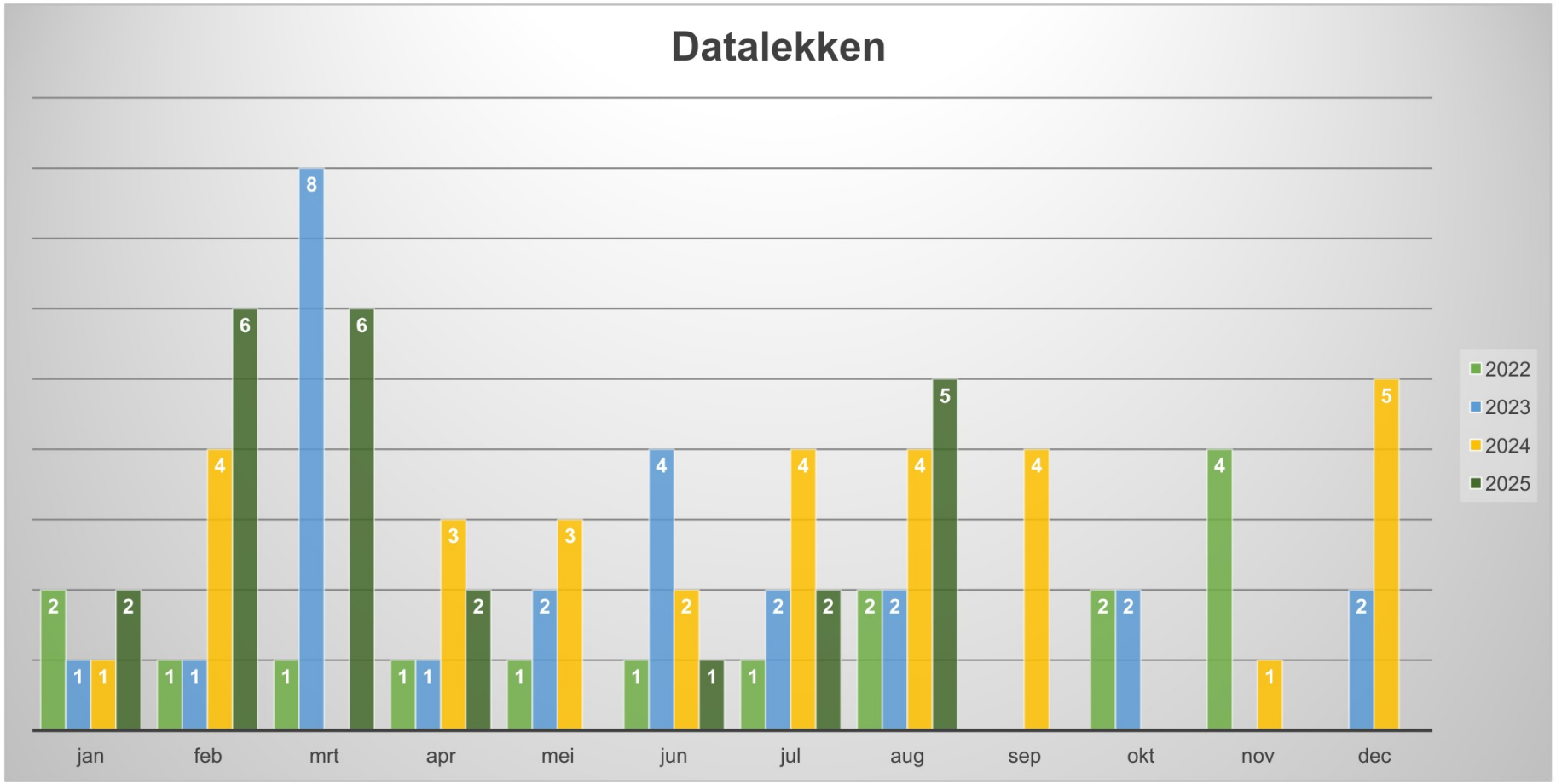
Hoe gaan we om met persoonsgegevens?

nationale ombudsman

- Hoe gaan wij om met persoonsgegevens? Privacybeleid
- Informatie voor burgers Privacyverklaring website
- Informatie voor werknemers Informatieblad AVG voor medewerkers

Datalekken
overzicht van de afgelopen 4 jaar

nationale ombudsman



Datalekken
meest voorkomende situaties

nationale ombudsman

- E-mails naar verkeerde ontvangers
  - Let op! Outlook vult een adres automatisch aan met autocomplete.
  - Hou de lijst van ontvangers beperkt (wie moet de informatie écht ontvangen?)
- Brieven naar verkeerde (oude) adressen
  - Indien mogelijk, controleer vooraf of het adres nog actueel is.
  - Controleer of het adres juist op de brief staat.
  - Verstuur brieven met bijzondere persoonsgegevens aangetekend.

Datalekken
melden van een (vermoedelijk) datalek

nationale ombudsman

- Via NoHow (voorkeur)
- Direct naar
- Vul het formulier in
- PO neemt contact op
- Meld een datalek direct, in ieder geval binnen 24 uur na ontdekking
- Verzoek onterechte ontvanger om vernietiging/retour van mail/brief

AVG-verzoeken
indiening en herkenning van een verzoek

nationale ombudsman

- Elke burger heeft een aantal rechten t.a.v. zijn persoonsgegevens, waaronder inzagerecht en recht op verwijdering.
- Verzoeker wordt via onze website (privacyverklaring) verzocht om een AVG-verzoek in te dienen via e-mail AVG@nationaleombudsman.nl of per post.
- AVG-verzoek in jouw dossier? Neem contact op met de PO via AVG@nationaleombudsman.nl

- Hoe herken je een AVG-verzoek?
  - “Ik wil inzage in (persoons)gegevens op basis van de AVG…”
  - “Welke (persoons)gegevens hebben jullie over mij?”
  - “Ik wil verwijdering van mijn (persoons)gegevens”

AVG inzageverzoek
Behandeling van het verzoek

nationale ombudsman

- PO coördineert en behandelt verzoek
- Verifiëren verzoek en scope
- Betrokken medewerkers worden geraadpleegd
- Persoonsgegevens worden verzameld in een overzicht /Stukken worden verzameld en geanonimiseerd
- Eindcontrole door FG en eventueel betrokken medewerkers
- Behandeltermijn:
  - 1 maand
  - Mogelijkheid om te verlengen met maximaal 2 maanden in geval inzageverzoek complex of veelomvattend is

Verwerken van persoonsgegevens

nationale ombudsman

- Sla stukken/documenten op één plek op
  - Voorkom dat informatie op verschillende plekken is opgeslagen.
- Communiceer professioneel
  - Dus voorkom meningen of kwalificaties (‘die lastige klager heeft weer gemaild, hij blijft maar doorzeuren’)
- Beperk persoonsgegevens in social media of berichtenapps
  - Deze informatie wordt soms buiten Europa opgeslagen.
- Sla persoonsgegevens niet langer op dan noodzakelijk
  - alleen die gegevens op die echt noodzakelijk zijn voor het behandelen van een klacht en knip eventueel pagina’s uit een pdf en gooi de rest weg.

Verzoek tot verwijderen van gegevens

nationale ombudsman

- Een verzoek tot verwijderen van gegevens wordt vaak gehonoreerd op het moment dat de verwerking op basis van ‘toestemming’ is.
  - Inschrijven voor een nieuwsbrief
  - Foto’s bij een evenement
- Voor klachtbehandeling maken we gebruik van de grondslag ‘wettelijke taak’. Bij deze grondslag is verwijderen van persoonsgegevens niet mogelijk, indien
  - We de persoonsgegevens conform AVG hebben verwerkt (grondslag, dataminimalisatie, voldoende waarborgen voor beveiliging/bescherming)
  - De bewaartermijn van een zaak nog niet verstreken is.

Heb je een AVG/privacy vraag?

nationale ombudsman

Stel deze aan:

- AVG-vertegenwoordiger: eerste aanspreekpunt
- Privacy Officer (PO)

Rol Functionaris Gegevensbescherming (FG):

- interne toezichthouder en adviserende rol

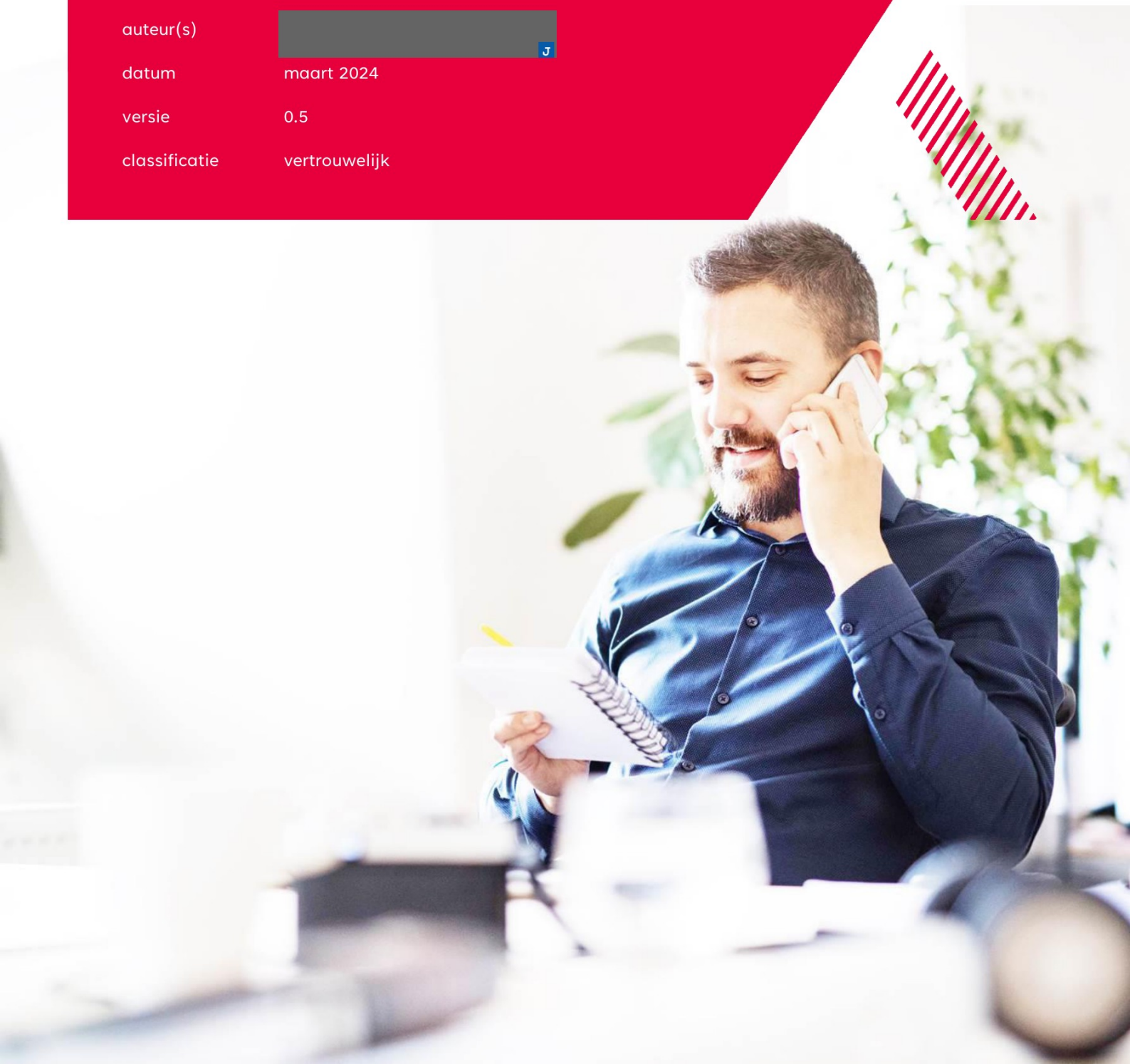
- Overzicht rollen NoHow

ilionx
experts in eenvoud

nationale ombudsman
als het misgaat tussen u en de overheid

Rapportage Fase 1 en Plan van Aanpak Fase 2 Nationale ombudsman

auteur(s)	[redacted]
datum	maart 2024
versie	0.5
classificatie	vertrouwelijk



Contents

3. Plan van Aanpak Fase 2

In dit hoofdstuk hebben we de aanpak voor Fase 2 uiteengezet zoals wij die voor ons zien. We nemen dit voorstel graag met jullie door om tot een gezamenlijk plan te komen die in lijn is met de verwachtingen en mogelijkheden.

Gezien de resultaten van Fase 1, willen we beginnen in Fase 2 met het Thema ‘Veilig werken op Kantoor’. We willen graag vanuit de kantoorbasis starten en met aankleding in het pand het Security Awareness programma goede zichtbaarheid geven. We behandelen in algemene zin ‘wat verstaan we onder veilig werken’ en ‘waarom is dit belangrijk/waarom vindt de Nationale ombudsman dit belangrijk’. En we gaan specifieker in op ‘wat we verstaan onder veilig werken op kantoor’; waarbij we zowel kennis-informatie bijbrengen als oefenen met situaties kunnen inschatten.
Daarna volgt het thema ‘Veilig werken onderweg’. Werken in de trein, buiten in de tuin, terras of de laptop mee op vakantie. Aan het einde van de zomerperiode starten we met thema ‘Veilig thuiswerken’. Waar moet je op letten bij het thuiswerken? Wat zijn de regels vanuit de NO? En waar moet je alert op zijn tijdens de drukke decembermaand.

Per thema komt materie van de volgende categorieën aan bod, [redacted]:

- Passwords, authenticatie en toegangsrechten
- Omgaan met sociale media
- Incidenten rapporteren

- Cybersecurity
- Privacy
- AVG
- Mobiele apparaten
- Internet gebruik
- Email security

Hierbij nog het overzicht en de opbouw zoals in de offerte opgenomen was, waarbij we langer nodig hebben gehad voor Fase 1. Fase 2 en 3 blijven nog steeds een duur van ieder 10 maanden hebben.

Security Awareness Programma Nationale Ombudsman

Fase 1 – 4 maanden

- Kick off bijeenkomst projectgroep
- Cyber Crisis Preparedness Training
- Kennis- en Cultuur Survey
- Interviews
- Achtergrondonderzoek en Deskresearch
- Phishing simulatie
- Assessment locatie rapport
- Analyse, rapportage, Plan van Aanpak Fase 2

Fase 2 – 10 maanden

- Thema Thuiswerken [3 maanden]
- Thema Werken op Kantoor [3 maanden]
- Thema Werken Onderweg [3 maanden]
- Kennis- en Cultuur Survey
- Analyse, rapportage, Plan van Aanpak Fase 3

Fase 3 – 10 maanden

- Thema Thuiswerken [3 maanden]
- Thema Werken op Kantoor [3 maanden]
- Thema Werken Onderweg [3 maanden]
- Kennis- en Cultuur Survey
- Analyse, rapportage, vervolgadvies

Per thema rollen we uit:

- Communicatiecampagne begeleiding (nieuwsbericht, gouden regels, wist-je-dat items etc.)
- Link naar relevant beleid
- Webinars: 5 x 45 minuten toegankelijk en relevant voor alle medewerkers. We behandelen NO-werkscenario's in de webinars (interactief).
- Phishing simulatie
- Flash Quiz

Per thema komt materie van deze categorieën aan bod:

- Cybersecurity
- Privacy
- AVG
- Omgaan met sociale media
- Paswoorden, authenticatie en toegangsrechten
- Incidenten rapporteren
- Mobiele apparaten
- Internet gebruik
- Email security

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

N Art. 5.1 lid 2 sub i

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen

ilionx
experts in eenvoud

nationale ombudsman
als het misgaat tussen u en de overheid

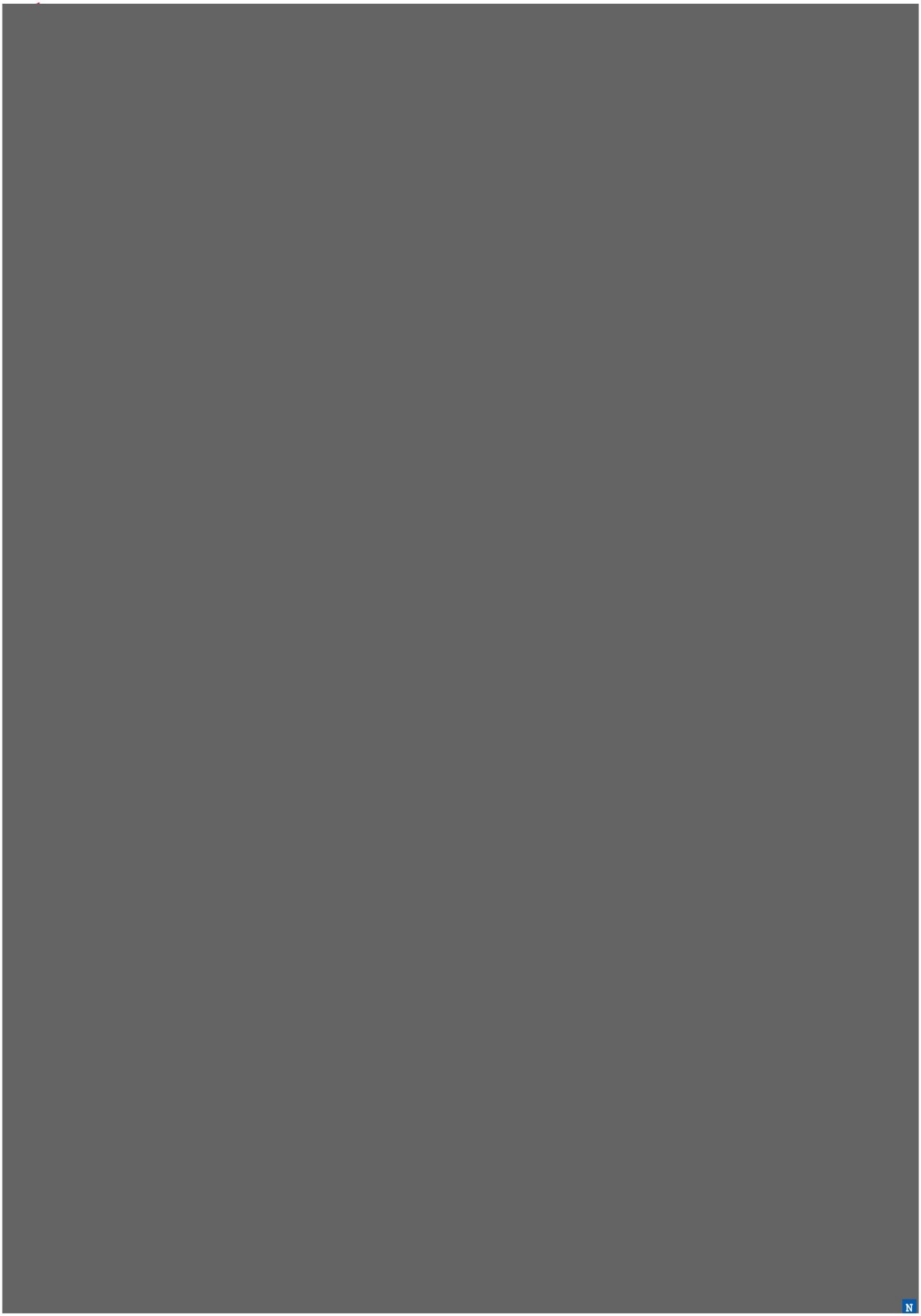
Rapportage Fase 2 en Plan van Aanpak Fase 3 Nationale ombudsman

auteur(s) [redacted]

datum 8 augustus 2025

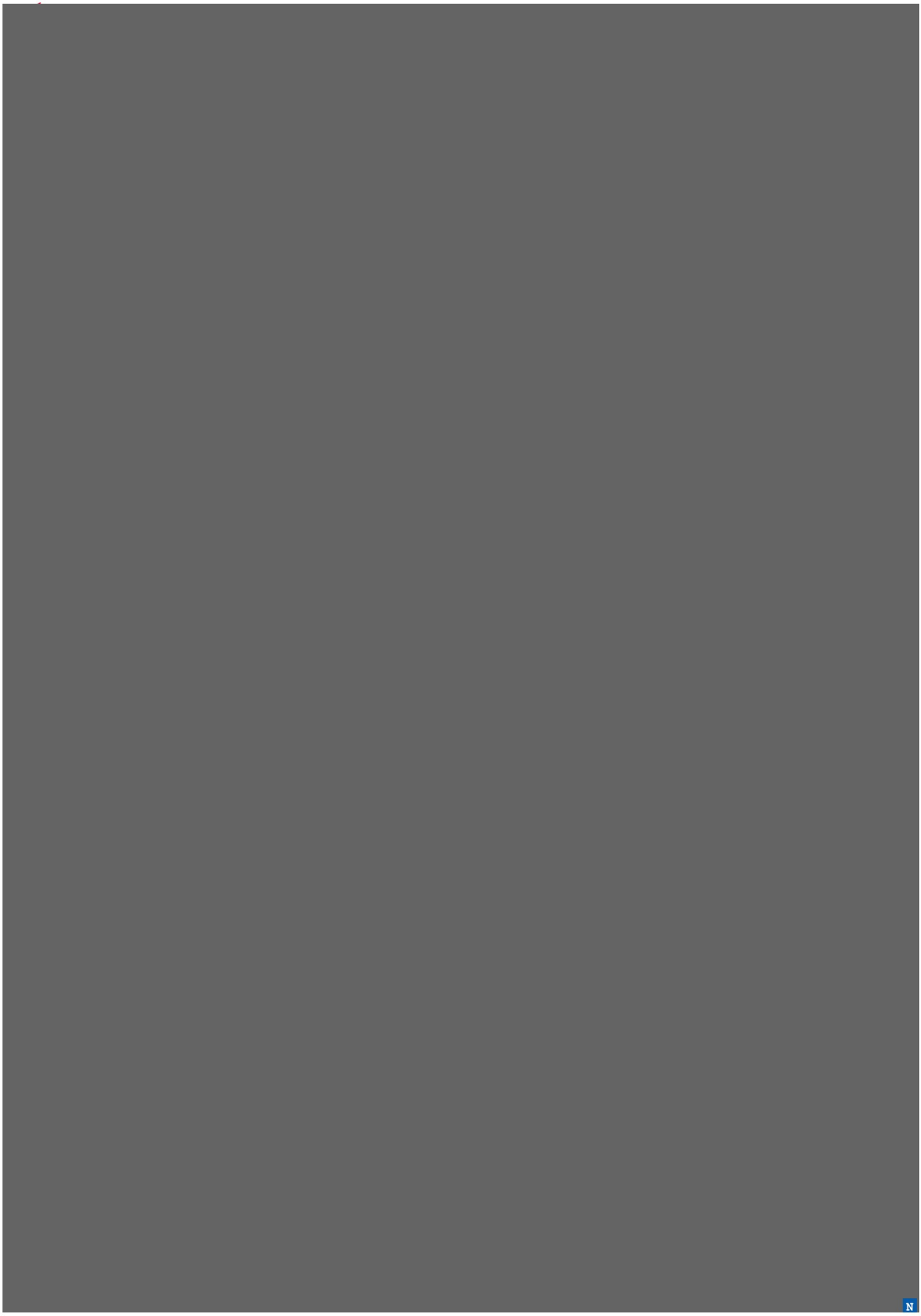
versie 1.0

classificatie vertrouwelijk



ilionx
experts in eenvoud

Contents



5. Plan van Aanpak Fase 3

In dit hoofdstuk hebben we de aanpak voor Fase 3 uiteengezet in een schema.

Hierbij nog het overzicht en de opbouw zoals in de offerte opgenomen was, waarbij we langer nodig hebben gehad voor Fase 1 en ook in Fase 2 hebben we de go-live van de campagne in de organisatie verschoven tot na de zomer van 2024 zodat voorbereidingen voor communicatie en het beeldmerk gereed was.

Security Awareness Programma Nationale Ombudsman

Fase 1 – 4 maanden

- Kick off bijeenkomst projectgroep
- Cyber Crisis Preparedness Training
- Kennis- en Cultuur Survey
- Interviews
- Achtergrondonderzoek en Deskresearch
- Phishing simulatie
- Assessment locatie rapport
- Analyse, rapportage, Plan van Aanpak Fase 2

Fase 2 – 10 maanden

- Thema Thuiswerken [3 maanden]
- Thema Werken op Kantoor [3 maanden]
- Thema Werken Onderweg [3 maanden]
- Kennis- en Cultuur Survey
- Analyse, rapportage, Plan van Aanpak Fase 3

Fase 3 – 10 maanden

- Thema Thuiswerken [3 maanden]
- Thema Werken op Kantoor [3 maanden]
- Thema Werken Onderweg [3 maanden]
- Kennis- en Cultuur Survey
- Analyse, rapportage, vervolgadvies

Per thema rollen we uit:

- Communicatiecampagne begeleiding (nieuwsbericht, gouden regels, wist-je-dat items etc.)
- Link naar relevant beleid
- Webinars: 5 x 45 minuten toegankelijk en relevant voor alle medewerkers. We behandelen NO-werkscenario's in de webinars (interactief).
- Phishing simulatie
- Flash Quiz

Per thema komt materie van deze categorieën aan bod:

- Cybersecurity
- Privacy
- AVG
- Omgaan met sociale media
- Paswoorden, authenticatie en toegangsrechten
- Incidenten rapporteren
- Mobiele apparaten
- Internet gebruik
- Email security

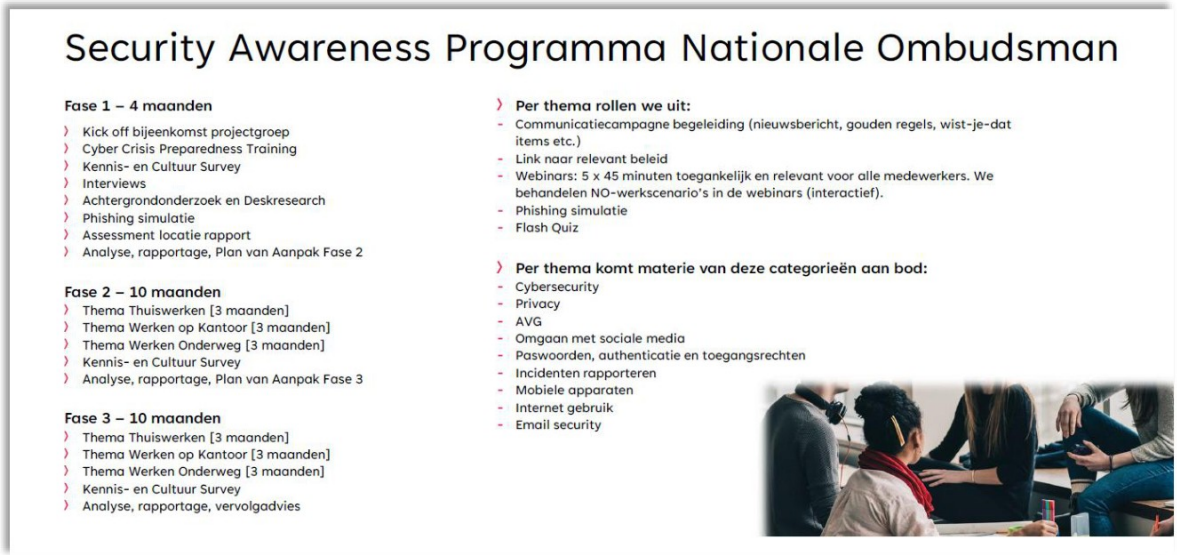
Doelen voor Fase 3:

- Goede samenwerking met projectteam
- Goede samenwerking met communicatie van de Nationale ombudsman
- Goede samenwerking met de teammanagers/leidinggevenden
- Goede participatie aan de webinars en quizzen: 75% en hoger
- Een daling in kliks op de phishing simulaties en een daling in het aantal medewerkers die vervolgens gevoelige gegevens achterlaten
- Een stijging in snelheid en hoeveelheid meldingen op de phishing simulaties
- Dat de meerderheid een voldoende scoort (70% en hoger) bij het maken van de quizzen
- SAPA kennisenquête score verbeteren: participatie en inhoudelijk op de onderwerkpen (t.o.v. de SAPA kennisenquête in Fase 1)
- Betrokken medewerkers die het onderwerp en de aanpak leuk en interessant vinden

Voorstel webinars security awareness fase 3.

Inleiding

Om bewustwording van informatiebeveiliging te vergroten wordt van zomer 2024 tot en met april 2026 een security awareness programma uitgevoerd: Veilig werken bij de ombudsman'. Inmiddels is fase 2 afgerond en kan fase 3 van start gaan.



In het projectteam is nagedacht over de opzet van fase 3, waarbij de volgende overwegingen een rol hebben gespeeld:

- De mix van webinars, tests en phishing simulatie bevalt goed.
- De opzet van de webinars aantrekkelijk houden en meer laten aansluiten op onze organisatie.
- Om de inhoud interessant te houden andere thema's kiezen
- Het doel aanscherpen:
    - goede participatie aan de webinars en quizzen: 95% en hoger
    - een daling in kliks op de phishing simulaties t.o.v. fase 2
    - een daling in het aantal medewerkers die vervolgens gevoelige gegevens achterlaten t.o.v. fase 2.
    - een stijging in snelheid en hoeveelheid meldingen op de phishing simulaties t.o.v. fase 2.
    - dat de meerderheid (85% en hoger) een ruim voldoende scoort (7 of hoger) bij het maken van de quizzen

Hoe bereiken we wat we willen bereiken?

We willen de gebruikelijke middelen inzetten met de volgende accenten (genoemde tijdstippen zijn onder voorbehoud van akkoord directie).

Communicatiecampagne

- De aankondiging van een volgende fase van Veilig werken bij de ombudsman wordt per mail verstuurd door de directie, waarbij de urgentie op de onderwerpen opnieuw wordt aangekaart en de data van de webinars van de tweede thema’s wordt gedeeld. De timing van deze mail is eind

september (begin oktober), ongeveer een maand voordat het eerste thema met webinars start zodat medewerkers lang van tevoren op de hoogte worden gesteld.
- Er worden periodiek No-How en/of Narrowcasting berichten geplaatst om continue aandacht te besteden aan specifieke informatiebeveiliging en privacy onderwerpen. Denk daarbij aan de onderwerpen;
    - Bewust printen en veilig papieren informatie weggooien. Mogelijkheid tot aanschaf van een papierversnipperaar thuis;
    - Veilig werken onderweg en mogelijkheid tot aanschaf van een privacyfilter;
    - Clear screen en clear desk beleid, en ongewenst gedrag ten aanzien van het onnodig bezet houden van werkplekken;
    - Het gebruik van wachtwoordmanager Keepass;
    - Datalekken in de organisatie.

Phishing simulaties

Tijdens Fase 3 zetten we opnieuw phishing simulaties uit naar alle medewerkers. Doelstelling is dat steeds minder medewerkers in de gesimuleerde phishing e-mails trappen en dat er sneller en meer gemeld wordt. In Fase 3 gaan we realistischer phishing toepassen. We zullen vaker phishingmails versturen, waarbij op willekeurige momenten een deel van de medewerkers verschillende phishingmails ontvangen. Zo krijgen de medewerkers niet allemaal op één moment dezelfde phishingmail.

- 4 phishing emails in de periode november 2025 t/m december 2025
- 4 phishing emails in de periode januari 2025 t/m februari 2026

Na elke phishing email ontvangen de medewerkers binnen enkele dagen opnieuw een email met daarin uitleg over dat het een simulatie betrof en hoe zij phishing hadden kunnen herkennen.

Quizzen

- Na de eerste reeks webinars (november 2025) zullen we een quiz uitsturen van circa 15 vragen. De quiz zal bestaan uit een mix van de materie dat tijdens het thema behandeld is.
- Na de tweede reeks webinars zullen we de SAPA-enquête uitsturen.

Directie en teammanagers

1. Dienen het juiste voorbeeld te geven voor veilig en bewust werken;
2. Dienen medewerkers aan te sporen voor het deelnemen aan de webinars en de kennisquizen en dragen zorg voor het behalen van de afgesproken participatie van 95%;
3. We vragen feedback op bij de teammanagers/leidinggevenden over hoe het onderwerp leeft binnen hun team, hoe het gaat met de participatie en motivatie. We luisteren om te kijken of en hoe we het SA-traject goed op de situatie aanpassen. En om de teammanagers/leidinggevenden handvatten te geven hoe de onderwerpen te behandelen binnen hun team.

Webinars

Om het kennis- en gedragsniveau op het gebied van informatieveiligheid en privacy bij de medewerkers te verhogen is het essentieel dat we op een creatieve en prikkelende manier aansluiten op het werk en de belevingswereld van de medewerkers. Dit vergroot de herkenning en maakt het opnemen en toepassen van de aangereikte kennis gemakkelijker. De webinars worden gegeven via Teams bijeenkomsten, ze duren ongeveer 60 minuten en we geven vier keer de webinar zodat er

voldoende mogelijkheid is voor iedereen om deel te nemen.

Thema's:

- **Aanvalsmethodes van cybercriminelen**. Op een interactieve, sprekende manier gaan we laten zien welke aanvalsmethodes vaak voorkomen en wat het effect is van de aanvalsmethodes. Concrete voorbeelden behandelen van bijv. gemeenten die getroffen zijn. Of een worst-case scenario uitwerken en behandelen voor wat er gebeurt als een succesvolle phishing aanval heeft plaatsgevonden.

- **Privacyvraagstukken in het dagelijks werk**. Bijvoorbeeld risico van foto's gebruiken in AI tooling. En een worst-case scenario uitwerken en behandelen voor wat er gebeurt als persoonsgegevens van een burger worden gelekt.

Hoe meten we de resultaten

- We houden bij wie deelnemen aan de training/webinars. Zo kunnen we zien wie wel/niet aanwezig is op individueel niveau maar kunnen dit ook op teamniveau uitsplitsen. En hier acties op ondernemen, zoals bijvoorbeeld die teamleiders/leidinggevenden medewerkers laten aansporen om deel te nemen.
- We maken een rapport op bij elke ronde phishing simulaties. Hieruit halen we of het omgaan met phishing verbetert: minder kliks en sneller melden. We kunnen ook uitsplitsen of telkens dezelfde mensen op phishing klikken of dat er een team is waar de klik percentage hoog ligt. We kunnen dan met elkaar kijken wat er aan de hand is en eventueel extra training inzetten. Wanneer de organisatie steeds adequater reageert op de phishing simulatie, dan kunnen we de phishing moeilijker maken.
- We maken een rapport op na de quiz. Zo kunnen we zien wie wel/niet de quiz heeft gemaakt en wat de resultaten zijn. Wanneer er minder goed wordt gescoord, kunnen we overwegen delen van de materie te herhalen. En ook hierbij, wanneer we zien dat weinig deelname is, of structureel medewerkers/teams niet deelnemen, dan kunnen we daarop actie ondernemen.
- Aan het einde van Fase 3 zetten we weer de SAPA-enquête uit. We vergelijken de resultaten van Fase 1, Fase 2 en Fase 3.
- We willen graag de beleving en het sentiment peilen bij de medewerkers na afloop van de webinar. Laagdrempelig maximaal 3 vragen. Forms formulier in de chat zetten en in de laatste minuten laten invullen. Zo kunnen we wat we aanbieden nog beter laten aansluiten op de beleving van de medewerker.

Vraagstelling

- De inhoud en opzet van fase 3;
- Het bijstellen van de KPI voor deelname van 85% naar 95% in het security & privacy awareness beleid met ingang van fase 3;
- Het organiseren van de webinars in november en februari;
- Hoe wordt voldoende deelname aan de webinars en de andere activiteiten verzekerd?