PROTOCOL MELDEN EN REGISTREREN VAN DATALEKKEN

Onze organisatie loopt de volgende stappen door wanneer zich een beveiligingsincident heeft voorgedaan met gegevens. Tevens documenteert onze organisatie eventuele datalekken op de bijgaande lijst.

Stap 1 - Zijn de betreffende gegevens *persoonsgegevens*?

Een inbreuk is pas relevant voor de meldingsplicht van de AVG als het *persoonsgegevens* betreffen, oftewel betreffen het alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon? (artikel 4 lid 1 AVG)

Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

JA? > Ga naar Stap 2.
NEE? > Het betreft geen datalek in de zin van de AVG, dus er hoeft niet gemeld te worden.

Stap 2 - Zijn de gegevens per ongeluk of op onrechtmatige wijze vernietigd, verloren of gewijzigd?

Een voorbeeld hiervan is als gegevens zoek zijn (USB-stick of smartphone zoek) of door onbevoegden zijn versleuteld (encrypted) of veranderd. (artikel 4 lid 12 AVG)

Indien onbevoegden gegevens met adequate encryptie buit maken, dan betreft het géén datalek mits de organisatie nog over een toegankelijke kopie van de gegevens beschikt.

JA? > Het betreft een datalek die gemeld moet worden. Ga naar Stap 5.
NEE? > Ga naar Stap 3.

Stap 3 - Zijn de gegevens ongeoorloofd verstrekt of ongeoorloofd toegankelijk geweest tot doorzenden, opslaan of op andere wijzen verwerken?

Ook als gegevens niet zijn verdwenen uit de eigen beschikking kan er soms sprake zijn van een datalek als onbevoegden de gegevens hebben kunnen raadplegen of anderszins verwerken. (artikel 4 lid 12 AVG)

Indien onbevoegden enkel toegang hadden tot versleutelde gegevens (met adequate encryptie), dan betreft het géén datalek.

JA? > Het betreft een datalek die gemeld moet worden. Ga naar Stap 5.
NEE? > Ga naar Stap 4.

Stap 4 - De onderhavige inbreuk dient gedocumenteerd te worden.

Ook als een inbreuk niet leidt tot een meldingsplicht, dienen deze te worden gedocumenteerd. Onze organisatie gebruikt hiervoor de hierna volgende registratielijst. (artikel 33 lid 5 AVG)

Stap 5 - Is het waarschijnlijk dat de inbreuk risico's inhoudt voor de rechten en vrijheden van natuurlijke personen?

De Meldingsverantwoordelijke – dit kan een functionaris gegevensbescherming (FG) zijn – beoordeelt het risico van de inbreuk samen met de Directie en eventueel de betrokken technische personen (bijv. de systeembeheerder van de Verwerker). Eventueel wordt een Externe Adviseur ingeschakeld bij twijfelgevallen of voor de begeleiding van het doen van de melding. De te beantwoorden vraag luidt: Is het waarschijnlijk dat de inbreuk in verband met de persoonsgegevens een risico inhoudt voor de rechten en vrijheden (lees hierin vooral de 'bescherming van de persoonlijke levenssfeer') van *natuurlijke* personen (dat zijn 'mensen' en géén *rechts*personen).

JA? > Er moet gemeld worden aan de Autoriteit Persoonsgegevens. Ga ook door naar Stap 6.

NEE? > De inbreuk is niet ernstig genoeg om te moeten worden gemeld. Registreer de inbreuk echter wel als vermeld onder Stap 4.

Hieronder een overzicht van voornoemde actoren van onze organisatie bij datalekken: ***(invullen)***

Actoren	**Naam**	**Telefoonnummer**	**E-mailadres**
Meldingsverantwoordelijke	R.A. Hoekstra	06-22136164	info@accountantswerk.nl
Datalek compliancefunctionaris	R.A. Hoekstra	06-22136164	info@accountantswerk.nl

Melden bij de Autoriteit Persoonsgegevens wordt gedaan via:
https://datalekken.autoriteitpersoonsgegevens.nl/
Let op: Indien met vertraging (na 72 uur) gemeld wordt, dient de vertraging te worden gemotiveerd.

Stap 6 - Houdt de inbreuk een *hoog* risico in voor de rechten en vrijheden van natuurlijke personen?

De Meldingsverantwoordelijke – dit kan een functionaris gegevensbescherming (FG) zijn – beoordeelt het risico van de inbreuk samen met de Directie en eventueel de betrokken technische personen (bijv. de systeembeheerder van de Verwerker). Eventueel wordt een Externe Adviseur ingeschakeld bij twijfelgevallen of voor de begeleiding van het doen van de melding.

Bij deze vraag is de situatie voor de betrokkene meer prangend en dient ook direct aan de betrokkene te worden gemeld, bijvoorbeeld om zijn wachtwoord te resetten of andere maatregelen te nemen om zoveel mogelijk schade te voorkomen. Raadpleeg de 'Beleidsregels

meldplicht datalekken' van de Autoriteit Persoonsgegevens hierover:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

JA? > Er moet *onverwijld* gemeld worden aan de betrokkene. Registreer de inbreuk ook als vermeld onder Stap 4.
NEE? > Er hoeft enkel aan de Autoriteit gemeld te worden (Stap 5).

Melding datalekken
Bij een melding aan de Autoriteit Persoonsgegevens moeten de volgende gegevens worden medegedeeld:
- de aard van het datalek, indien mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en de contactgegevens van de functionaris voor de gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het datalek;
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Als het niet mogelijk is om al deze informatie in één keer te verstrekken, dan mag de informatie ook in stappen worden verstrekt, mits dat zonder onredelijke vertraging gebeurt. Verder is van belang dat de verwerkingsverantwoordelijke alle datalekken documenteert (o.a. de feiten, de gevolgen en de genomen maatregelen), zodat de Autoriteit Persoonsgegevens in staat wordt gesteld te controleren of de verwerkingsverantwoordelijke al dan niet ten onrechte geen melding heeft gedaan. De AVG vermeldt niet hoe lang deze gegevens bewaard moeten worden. Wij adviseren een bewaartermijn van twee jaar.

Wie moet de melding verrichten?

De AVG gaat ervan uit dat de verwerkingsverantwoordelijke de melding doet aan de Autoriteit Persoonsgegevens. De verwerker hoeft daarentegen geen melding te doen. Indien het datalek ontstaat bij de verwerker, dan moet de verwerker de verwerkingsverantwoordelijke daarover informeren en die doet op zijn beurt vervolgens de melding bij de Autoriteit Persoonsgegevens. Omdat het in het belang is van de verwerkingsverantwoordelijke om zo snel mogelijk op de hoogte te raken van een datalek bij de verwerker (vanwege de beperkte termijn om de melding aan de Autoriteit Persoonsgegevens te doen), is het van belang dat daarover heldere afspraken worden gemaakt in de verwerkersovereenkomst.

Hoe dient aan de Autoriteit Persoonsgegevens te worden gemeld?
De Autoriteit Persoonsgegevens heeft een digitaal loket voor het online melden van datalekken via een webformulier: https://datalekken.autoriteitpersoonsgegevens.nl/.

Meldplicht aan de betrokkene(n)?

Soms is een melding aan de Autoriteit Persoonsgegevens niet voldoende en moet de verwerkingsverantwoordelijke tevens de betrokke(n) op de hoogte stellen van het datalek (met alle risico's op verlies van reputatie van dien). Het uitgangspunt van de AVG is dat de betrokkene op de hoogte moet worden gesteld van het datalek, indien het datalek een hoog risico inhoudt voor de

rechten en vrijheden van betrokkenen. Echter, de mededeling aan de betrokkene is niet vereist wanneer één van deze voorwaarden is vervuld:

- de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop het datalek betrekking heeft, met name maatregelen die de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
- de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het risico voor de rechten en vrijheden van de betrokkenen zich waarschijnlijk niet meer zal voordoen;
- de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

Indien geen van deze voorwaarden van toepassing is, dan is het van belang dat de melding aan de betrokkene een duidelijke omschrijving bevat, in eenvoudige taal, van de aard van het datalek. Verder moet aan de betrokkene worden medegedeeld:

- de naam en de contactgegevens van de functionaris voor de gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het datalek;
- de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

REGISTRATIE VAN INBREUKEN

Zie hiertoe de losse Excel-sheet waarin bijgehouden wordt welke datalekken er geweest zijn.