PERFECT DAY
CYBER SECURITY

Datalek: melden of niet?

Stroomschema datalekprotocol

Heb je een datalek? Dan moet je dat in sommige gevallen melden bij de Autoriteit Persoonsgegevens (AP) en de betrokkenen. De regelgeving daarover is vrij complex en fouten kunnen je duur komen te staan. Om dat te voorkomen maakten wij een stroomschema. Dit helpt je te bepalen of je moet melden en bij wie.

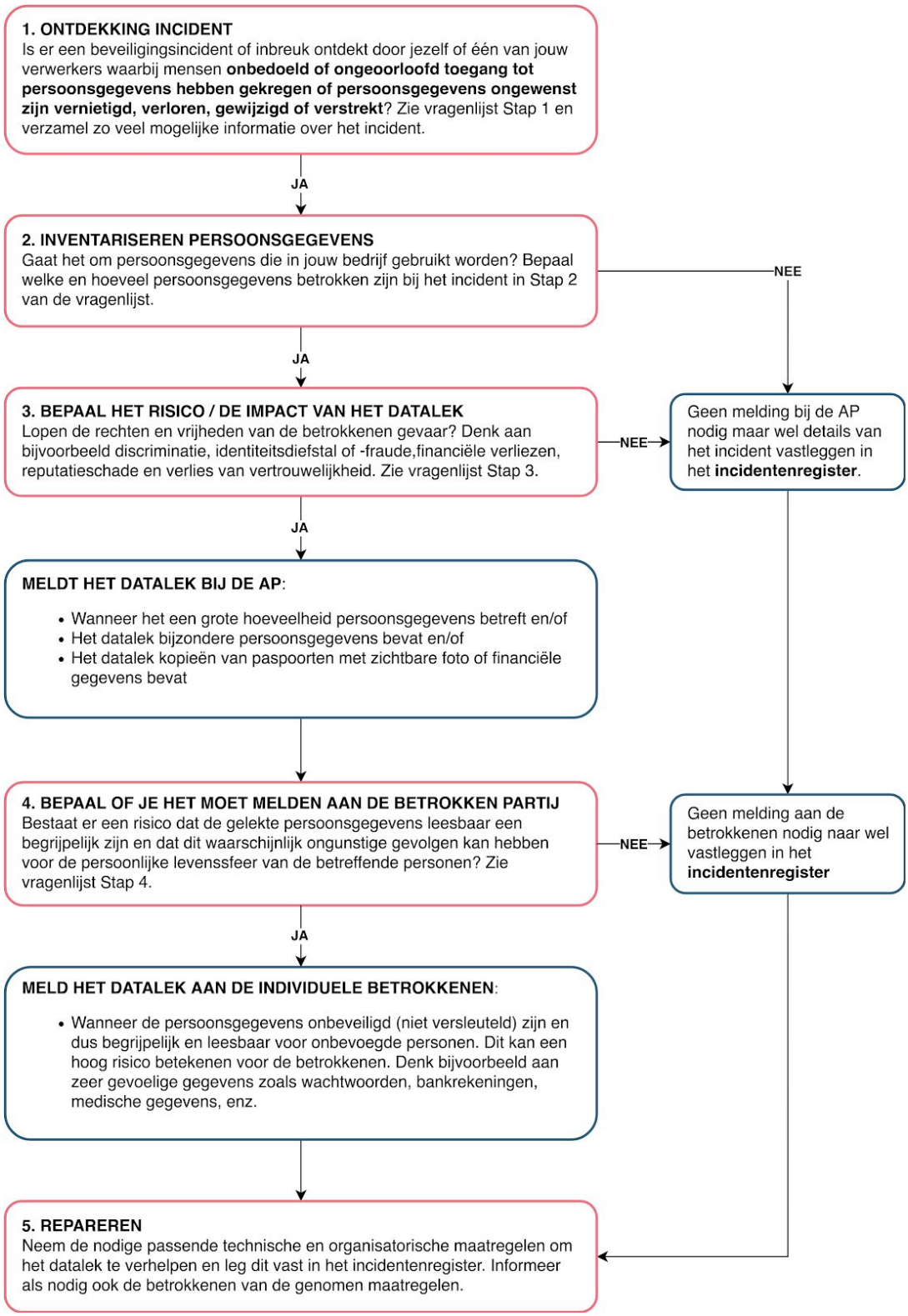
Wat is een datalek?

Allereerst is het van belang te definiëren waar we het over hebben als we spreken over een datalek. Technisch gezien treedt een datalek op wanneer "ongeoorloofde of onbedoelde toegang tot persoonsgegevens plaatsvindt." Maar ook door het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Hierdoor kunnen de betrokken personen namelijk schade leiden. Neem deze beschrijving super letterlijk. In sommige gevallen kan een e-mail die naar de verkeerde persoon wordt gestuurd al als datalek beschouwd worden. Verderop lees je hier meer over.

Hulp en uitleg

Achter het stroomschema vind je hulp en uitleg om de verschillende fases beter te kunnen toepassen. De nummers in het stroomschema refereren naar de nummers in de uitleg. Daar staat dan meer informatie over de stap in het stroomschema.

Wil je meer weten? Wij helpen je graag! Je kunt ons bereiken op nummer 085-048 6109 of via contact@perfectday.nl.


1. ONTDEKKING INCIDENT
Is er een beveiligingsincident of inbreuk ontdekt door jezelf of één van jouw verwerkers waarbij mensen onbedoeld of ongeoorloofd toegang tot persoonsgegevens hebben gekregen of persoonsgegevens ongewenst zijn vernietigd, verloren, gewijzigd of verstrekt? Zie vragenlijst Stap 1 en verzamel zo veel mogelijke informatie over het incident.
JA
2. INVENTARISEREN PERSOONSGEGEVENS
Gaat het om persoonsgegevens die in jouw bedrijf gebruikt worden? Bepaal welke en hoeveel persoonsgegevens betrokken zijn bij het incident in Stap 2 van de vragenlijst.
NEE
JA
3. BEPAAL HET RISICO / DE IMPACT VAN HET DATALEK
Lopen de rechten en vrijheden van de betrokkenen gevaar? Denk aan bijvoorbeeld discriminatie, identiteitsdiefstal of -fraude,financiële verliezen, reputatieschade en verlies van vertrouwelijkheid. Zie vragenlijst Stap 3.
NEE
Geen melding bij de AP nodig maar wel details van het incident vastleggen in het incidentenregister.
JA
MELDT HET DATALEK BIJ DE AP:
• Wanneer het een grote hoeveelheid persoonsgegevens betreft en/of
• Het datalek bijzondere persoonsgegevens bevat en/of
• Het datalek kopieën van paspoorten met zichtbare foto of financiële gegevens bevat
4. BEPAAL OF JE HET MOET MELDEN AAN DE BETROKKEN PARTIJ
Bestaat er een risico dat de gelekte persoonsgegevens leesbaar een begrijpelijk zijn en dat dit waarschijnlijk ongunstige gevolgen kan hebben voor de persoonlijke levenssfeer van de betreffende personen? Zie vragenlijst Stap 4.
NEE
Geen melding aan de betrokkenen nodig naar wel vastleggen in het incidentenregister
JA
MELD HET DATALEK AAN DE INDIVIDUELE BETROKKENEN:
• Wanneer de persoonsgegevens onbeveiligd (niet versleuteld) zijn en dus begrijpelijk en leesbaar voor onbevoegde personen. Dit kan een hoog risico betekenen voor de betrokkenen. Denk bijvoorbeeld aan zeer gevoelige gegevens zoals wachtwoorden, bankrekeningen, medische gegevens, enz.
5. REPAREREN
Neem de nodige passende technische en organisatorische maatregelen om het datalek te verhelpen en leg dit vast in het incidentenregister. Informeer als nodig ook de betrokkenen van de genomen maatregelen.

DATALEK PROTOCOL: TOELICHTING & HULP VRAGENLIJST

Algemeen

Je hoeft niet alle datalekken bij de Autoriteit Persoonsgegevens (AP) te melden. In grote lijnen komt het er op neer dat je moet melden als een datalek het mogelijk maakt om mensen op individueel niveau te identificeren en ze door de aard van de gelekte data schade kunnen lopen. Denk bijvoorbeeld aan identiteitsdiefstal, discriminatie, financiële of reputatieschade.

Technisch gezien treedt een datalek wanneer "ongeoorloofde of onbedoelde toegang tot persoonsgegevens plaatsvindt." Maar ook door het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Hierdoor kunnen de betrokken personen namelijk schade leiden.

Er zijn drie mogelijke acties na een inbreuk:

1. **Geen melding nodig** (geen of laag risico)
2. **Melding alleen bij de AP** (risico is wel aanwezig)
3. **Melding zowel bij de AP als bij de betrokkenen**

Melden binnen 72 uur

Als er melding moet worden gedaan, dan moet dat binnen 72 uur na ontdekking van het incident plaatsvinden. Meldingsformulier en procedure zijn te vinden bij https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken

Twijfel je?

De melding bij de AP is maar een onderdeel van het hele datalek protocol. Een onderzoek naar het datalek kan verder doorgaan na de melding. Ook kunnen bestaande meldingen aangepast worden of zelfs geheel ingetrokken worden als bij nader onderzoek blijkt dat er geen risico bestaat voor de betrokkenen. Op de site van de AP zijn beide procedures in kaart gebracht. In het algemeen bij twijfel geldt de regel: **beter het datalek aan de AP melden en/of Perfect Day raadplegen.**

De volgende zaken zijn relevant bij de risicobeoordeling:

- Het type inbreuk
- Ernst van de gevolgen voor individuen
- Gemakkelijke identificatie van individuen
- Bijzondere kenmerken (bijv. kinderen of andere kwetsbare individuen)
- De opgenomen persoonsgegevens (zoals naam, adres, bankgegevens, biometrie, enz.)

- Het volume van de betrokken gegevens
- Het aantal betrokkenen
- Zijn de persoonsgegevens (voldoende complex) versleuteld

Stappenplan

Hieronder vind je een aantal vragen per stap. Hiermee helpen we je:

1. Het beveiligingsincident op een juiste manier te registreren
2. Het datalek op een juiste manier te registreren
3. Te bepalen of je het incident moet melden bij de AP en betrokken personen

STAP 1: INCIDENT ONTDEKKEN / REGISTREREN

Hoe ontstaat een datalek? Dat kan op heel veel manieren. Om je een beeld te geven vind je hieronder 4 veel voorkomende situaties:

1. Diefstal of verlies van apparaten (laptops, tablets, smartphones) en geheugendragers (zoals USB sticks, externe harde schijven, CD/DVD). In tegenstelling tot wat veel mensen denken is er ook sprake van een datalek als fysieke documenten of dossiers gestolen of verloren raken .
2. Een digitale aanval op je netwerk zoals ransomware, phishing, de aanwezigheid van virussen of andere soorten malware die gericht zijn op het stelen van gegevens.
3. Het onbedoeld mailen of versturen van persoonsgegevens aan derde partijen die deze gegevens niet hadden moeten ontvangen.
4. Toegang tot gevoelige gegevens door medewerkers die daar niet toe bevoegd zijn.

Let op: Zodra je een incident waarneemt, registreer dan zo veel mogelijk details over het incident. De registratie staat los van de beslissing om wel of niet te melden bij de AP en moet altijd gebeuren. Registreer de details van het incident met behulp van deze vragen:

- Wanneer heb je de inbreuk ontdekt? Datum + Tijd
- Wanneer heeft de inbreuk vermoedelijk plaatsgevonden? Datum + Tijd
- Hoe ben je op hoogte van de inbreuk gekomen?
- Wat is er gebeurd? Registreer zoveel mogelijk over wat er gebeurd is, wat er is misgegaan en hoe het gebeurd is.
- De aard van de inbreuk: bijvoorbeeld diefstal, onbedoelde vernietiging, openbaarmaking of geen technische details beschikbaar
- Is de inbreuk veroorzaakt door een cyberincident? Ja / Nee / Weet niet

BELANGRIJK: Gaat het om persoonsgegevens van jouw bedrijf die worden verwerkt of opgeslagen bij derde partijen (verwerkers), zoals bijvoorbeeld een clouddienst? Dan is die partij verplicht het incident direct aan jou te melden maar jij moet zelf melding doen bij de AP (als dat nodig is).

STAP 2: INVENTARISEREN VAN PERSOONSGEGEVENS

Bepaal of de gelekte gegevens persoonsgegevens zijn en wat voor type. Bepaal ook wie de betrokkenen (groep personen) zijn bij de inbreuk. Wees zo volledig mogelijk en als het niet bekend is wat er precies gelekt is, leg dat dan ook vast. Hieronder volgen voorbeelden van mogelijke persoonsgegevens, maar registreer ook eventuele andere persoonsgegevens.

- Persoonsgegevens zoals:
    - Basis persoonlijke identificatiegegevens bijv. naam, adres, woonplaats
    - Identificatiegegevens bijv. gebruikersnamen, wachtwoorden
    - Locatie gegevens zoals IP-adressen
    - Economische en financiële gegevens bijv. creditcardnummers, bankgegevens
    - Officiële documenten bijv. rijbewijzen, scan paspoorten, geboorte of huwelijkse aktes, kentekens, KvK Nummers, etc.
    - CV's / Diploma's / Certificaten
    - Andere persoonsgegevens

- Bijzondere persoonsgegevens zoals:
    - Gegevens die raciale of etnische afkomst onthullen
    - Politieke opvattingen
    - Religieuze of filosofische overtuigingen
    - Vakbondslidmaatschap
    - Gegevens over seksleven, seksuele geaardheid en/of geslachtsverandering
    - Medische en/of gezondheidsgegevens
    - Genetische of biometrische gegevens (o.a. vingerafdrukken, stem, handschrift, scans van netvlies, iris en/of gelaat, DNA)
    - Strafrechtelijke veroordelingen en/of overtredingen
    - Andere persoonsgegevens

BELANGRIJK: Wanneer het datalek bijzondere persoonsgegevens bevat of kopieën van paspoorten met zichtbare foto of financiële gegevens (schulden, salarisgegevens, etc) bevat moet altijd een melding bij de AP gedaan worden.

- Categorieën van persoonsgegevens die in de inbreuk zijn opgenomen (weer zo volledig mogelijk)
    - Medewerkers, stagiairs, inhuur, oproepkrachten, etc.
    - Klanten of potentiële klanten
    - Leveranciers van goederen en diensten
    - Partners in de bedrijfsvoering
    - Gebruikers
    - Abonnees
    - Patiënten
    - Minderjarigen
    - Personen uit kwetsbare groepen
    - Andere categorieën

BELANGRIJK: Betreft het datalek kinderen of andere kwetsbare personen? Dan zul je het moeten melden bij de AP en zeer waarschijnlijk ook bij de betrokkene(n)

Bepaal, indien mogelijk, de hoeveelheid gegevens en het aantal betrokken personen:

- Is het aantal betrokkenen bekend? Hoeveel? Ja / Nee
- De hoeveelheid (volume) van de betrokken gegevens. Hoeveel data is er betrokken bij de inbreuk (indien niet bekend maak een schatting)?

BELANGRIJK: Over het algemeen geldt: hoe meer personen er betrokken zijn, hoe groter de gevolgen van het datalek. Wij adviseren je altijd bij de AP te melden als je datalek betrekking heeft op meer dan 1.000 personen.

STAP 3: BEOORDEEL HET RISICO / IMPACT

Wat zijn de eventuele gevolgen van het datalek voor de levenssfeer van de betrokken personen? En hoe groot is dat risico? Bijvoorbeeld:

- Discriminatie
- Identiteitsdiefstal of -fraude
- Financiële verliezen
- Reputatieschade
- Verlies van vertrouwelijkheid
- Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen

Vragen:

- Wat is de kans dat betrokkenen aanzienlijke gevolgen zullen ervaren als gevolg van de inbreuk? Zeer waarschijnlijk / Waarschijnlijk / Neutraal / Onwaarschijnlijk / Niet waarschijnlijk / Onbekend
- Hoe groot is het risico dat een betrokkene ernstige schadelijke gevolgen heeft van het incident? Hoog risico / Wel een risico / Laag of geen risico
- Beschrijf, indien mogelijk, de gevolgen voor betrokkenen (vink aan alle keuzes). Bijvoorbeeld:
    - Gegevens zijn alleen openbaar gemaakt
    - Gegevens zijn gemodificeerd
    - Gegevens zijn niet meer toegankelijk (vergrendeld)
    - Gegevens zijn gestolen (permanent verlies)
    - Gegevens zijn gewist
    - Andere gevolgen
    - Dit is (nog) niet bekend

MELD HET DATALEK BIJ HET AP:

- **Wanneer het een grote hoeveelheid persoonsgegevens betreft en/of**
- **Het datalek bijzondere persoonsgegevens bevat en/of**
- **Het datalek kopieën van paspoorten met zichtbare foto of financiële gegevens bevat**

De Autoriteit Persoonsgegevens heeft zelf een document opgesteld met een aantal voorbeelden van datalekken en of deze wel of niet gemeld moeten worden: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2019_voorbeeldlijst_wel_niet_melden_datalek_def.pdf

Voor het uiteindelijk melden van een datalek ga je naar https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken.

STAP 4: MELDEN AAN DE BETROKKEN PARTIJ (BEVEILIGING VAN GEGEVENS)

Bij deze stap is het met name belangrijk om te bepalen of de persoonsgegevens toegankelijk waren tijdens het incident. Dat wil zeggen: leesbaar en begrijpelijk voor ontvangers die daar niet voor gemachtigd zijn.

Om de risico's voor de betrokkenen af te wegen is het cruciaal om te weten of de gegevens versleuteld waren en hoe sterk die versleuteling is. Als gelekte persoonsgegevens heel goed beveiligd of versleuteld

zijn, waardoor de data niet toegankelijk is voor anderen hoef je het datalek niet aan betrokken personen te melden.

Als de persoonsgegevens bij een inbreuk wel begrijpelijk en leesbaar zijn dan is het risico voor betrokkenen hoog. In de vorige stap heb je bepaald hoe ernstig de mogelijke gevolgen kunnen zijn. Zijn die mogelijk ernstig? Dan is een melding bij de AP en aan betrokkenen. De wet maakt overigens wel duidelijk dat informeren van de betrokkenen niet een onevenredige inspanningen moet vergen. Het moet technisch haalbaar zijn om de personen individueel op de hoogte te stellen van het incident en de mogelijke gevolgen. (Art. 34)

Vragen: (Heb je zelf niet alle antwoorden? Deze informatie is waarschijnlijk te achterhalen bij de IT-leverancier, clouddienstverlener, hostingpartij, etc)

- Zijn de persoonlijke gegevens versleuteld (onbegrijpelijk en/of ontoegankelijk)? Ja / Nee / Onbekend
- Wat is de sterkte van de gebruikte versleuteling (algoritmes, hashes, etc)?
- Zijn de sleutels voor de encryptie nog steeds veilig (niet in handen van onbevoegde personen)? Ja / Nee / Onbekend
- In hoeverre waren de gegevens gepseudonimiseerd (d.w.z. dat kenmerken van een individu niet meer te koppelen zijn aan zijn identiteit en niet meer identificeerbaar zijn)? Ja / Nee / Onbekend
- Bestaan er back-ups van de persoonsgegevens? Ja / Nee / Onbekend

BELANGRIJK: Als er passende technische maatregelen zijn genomen om de data te beschermen (de persoonsgegevens zijn ontoegankelijk of onbegrijpelijk gemaakt via bijvoorbeeld encryptie) dan is het risico voor betrokkenen verlaagd en dan vervalt de plicht om ze individueel te informeren.

LET OP: Als de betreffende persoonsgegevens al publiekelijk beschikbaar waren dan hoeft het datalek niet bij de Autoriteit Persoonsgegevens gemeld te worden.

DATALEK MELDEN AAN DE INDIVIDUELE BETROKKENEN

- **Persoonsgegevens zijn onbeveiligd (niet versleuteld) en dus begrijpelijk en leesbaar voor onbevoegde personen. Dit kan een hoog risico voor de betrokkenen betekenen. Denk bijvoorbeeld aan zeer gevoelige gegevens zoals wachtwoorden, bankrekeningen, medische gegevens, enz.**
- **Het datalek kan waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de persoon.**

STAP 5: REPAREREN

Na een incident word je geacht maatregelen te nemen om iets dergelijks in de toekomst te voorkomen. De oorzaak of omstandigheden waardoor het datalek is ontstaan moet verholpen worden. Vergeet niet om de maatregelen die je hebt genomen in het incidentenregister te benoemen. En vermeld ze ook als je een melding aan betrokkenen maakt. Zo benadruk je dat je het incident serieus neemt en de veiligheid van hun gegevens in de toekomst (beter) waarborgt.

Vragen:

- Welke passende technische en organisatorische maatregelen zijn er genomen om het incident aan te pakken?
- Indien van toepassing, zijn de betrokkenen over deze maatregelen geïnformeerd? Ja / Nee

Tot slot

Het doel van incidentenregister is dat je leert van eerdere datalekken om zo maatregelen te nemen en daarmee de kans op nieuwe incidenten verkleint. Een expert van Perfect Day helpt jou graag om de risico's van je bedrijf in kaart te brengen.

Over Perfect Day

Perfect Day is dé partij voor cyber & data security in het mkb. Je kunt bij ons terecht voor advies en oplossingen. Daarvoor brengen we altijd eerst het grote plaatje van jouw bedrijf in kaart. Dat bestaat uit techniek, medewerkers, processen en wetgeving (avg). We maken dreigingen en kwetsbaarheden inzichtelijk. En helpen ze aan te pakken. Met een effectieve mix van persoonlijk advies en de juiste producten. Praktisch, persoonlijk en betaalbaar.

Wil je meer weten? Wij helpen je graag! Je kunt ons bereiken op nummer 085-048 6109 of via mail: contact@perfectday.nl.