PROTOCOL MELDING DATALEKKEN

Versie 0.1

Inhoudsopgave:

1. Vooraf

Bij Stichting Fonds Collectieve Belangen voor de Pluimveeverwerkende Industrie (hierna: Stichting OFP) worden, zoals vrijwel overal, persoonsgegevens verwerkt. Dat betreft gegevens van onze medewerkers, partners, enzovoort. Uiteraard willen wij daar zeer zorgvuldig mee omgaan, om geen onnodige (of onnodig grote) inbreuk te maken op de privacy van de betrokken personen. Daartoe zijn we ook wettelijk verplicht. Op 25 mei 2018 is de AVG vervangen door een nieuwe Europese privacywet, de Algemene Verordening Gegevensbescherming (**AVG**).

Door zorgvuldig met persoonsgegevens om te gaan, beperken wij de kans op kwalijke gevolgen voor de betrokkenen, op mogelijke publicitaire schade voor Stichting OFP, en op (hoge) boetes van de Autoriteit Persoonsgegevens (**AP**; de Nederlandse privacy-toezichthouder).

Niettemin kan het altijd gebeuren dat er wat mis gaat, waardoor er persoonsgegevens verloren gaan of op 'op straat komen te liggen', door een menselijke fout, activiteiten van hackers of anderszins. Dan moeten er uiteraard zo snel mogelijk maatregelen worden genomen. Bovendien moet zo'n datalek in de meeste gevallen binnen 72 uur (!) na ontdekking worden gemeld bij de AP, en soms zelfs aan alle betrokken personen.

Om ervoor te zorgen dat Stichting OFP – op tijd – aan deze meldingsplichten kan voldoen, is dit protocol opgesteld. Het allerbelangrijkste kan in de volgende twee punten worden samengevat:

1. **Wees alert** op mogelijke problemen bij de verwerking van persoonsgegevens (dubieuze mails, niet-afgesloten laptops, vergeten afdrukken bij de printer, etc.), en

2. **Informeer zo snel mogelijk de Contactpersoon Privacy** bij een vermoeden van een onregelmatigheid met betrekking tot persoonsgegevens en neem zo mogelijk meteen maatregelen om het lek te stoppen en de eventuele gevolgen te beperken. De Contactpersoon Privacy bepaalt wat er dan verder moet gebeuren aan de hand van dit protocol. In § 2.2 staat hoe je hem kunt bereiken.

Deze twee punten moet je in elk geval kennen en toepassen, ook als je niet het héle protocol doorneemt (wat ongetwijfeld nuttig is, maar misschien niet voor iedereen even noodzakelijk).

Dit datalekkenprotocol is grotendeels gebaseerd op de huidige wet en de daarbij behorende Beleidsregels voor de melding van datalekken van de AP. De meeste schema's zijn ook hieraan ontleend. Deze Beleidsregels zijn te vinden op de website van de AP, via onderstaande URL:

https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

2. Protocol melding datalekken – algemeen

Na een korte inleiding bevat dit hoofdstuk de nodige gegevens met betrekking tot de Contactpersoon Privacy van Stichting OFP (§ 2.2) en een toelichting op de gebruikte begrippen (§ 2.3).

2.1. Inleiding

Mochten er in onze organisatie persoonsgegevens zijn gelekt, dan moeten we dit uiterlijk binnen 72 uur aan de Autoriteit Persoonsgegevens (AP) kunnen melden.

Wij hebben dit protocol opgesteld om risico's en incidenten met betrekking tot persoonsgegevens in een zo vroeg mogelijk stadium te herkennen en om vervolgens zo snel mogelijk de juiste acties te kunnen ondernemen. In dit protocol kan je lezen wat je moet doen bij constatering van een beveiligingslek, een beveiligingsincident of een datalek, en wat er dan verder moet gebeuren.

⇒ De eerste stap is altijd om de Contactpersoon Privacy op de hoogte te stellen, die wij hiervoor hebben aangesteld. Zie daarvoor hierna, § 2.2.

Daarnaast bevat het protocol in § 2.3 een toelichting op de gebruikte begrippen, zoals 'persoonsgegeven', 'verwerkingsverantwoordelijke', en 'verwerking van persoonsgegevens'.

Het eigenlijke protocol vind je dan in Hoofdstuk 3.

2.2. Contactpersoon Privacy

Zodra je vermoedt dat er sprake is of zou kunnen zijn van een mogelijk probleem met de beveiliging van persoonsgegevens, moet je onmiddellijk telefonisch met de Contactpersoon Privacy contact opnemen. Samen met de Contactpersoon worden dan de volgende stappen bepaald.

Dit geldt ook als je een dergelijke melding krijgt van één van onze verwerkers (zie § 2.3.8).

Bedenk, dat als er sprake is van een echt datalek, dit binnen 72 uur na ontdekking gemeld moet kunnen worden! Dat geldt ook als het datalek door een verwerker is ontdekt.

- De Contactpersoon Privacy is: [ ]
- De dienstdoende Contactpersoon Privacy is (7x24 uur) te bereiken via het crisisrooster
- Minder spoedeisende vragen en opmerkingen kunnen worden gemaild aan: privacy@szpluimvee.nl.

2.3. Toelichting op de gebruikte begrippen

In dit protocol wordt een aantal termen gebruikt die in de privacyregelgeving een speciale betekenis hebben, die wat kan afwijken van de betekenis in het normale spraakgebruik. De juiste interpretatie van deze begrippen is van belang voor de toepassing van het datalekkenprotocol. Hieronder een overzicht.

2.3.1. AVG / Algemene Verordening Gegevensverwerking

De AVG is de nieuwe Europese privacywet die op 25 mei 2016 is vastgesteld en die na een overgangsperiode van twee jaar op 25 mei 2018 in alle landen van de EU van toepassing is.

2.3.2. De Autoriteit Persoonsgegevens (AP)

De Autoriteit Persoonsgegevens (hierna verder AP) is de wettelijke toezichthouder op de naleving van de AVG en andere privacywetten in Nederland.

2.3.3. Persoonsgegevens

De AVG is alleen van toepassing op ‘persoonsgegevens’. Dat zijn gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Zeker met de huidige technologie en beschikbaarheid van (big) data, is een gegeven al snel een persoonsgegeven. Het wordt immers steeds makkelijker om een gegeven tot iemand te herleiden, ook als dat op het eerste gezicht geen persoonsgegeven lijkt te zijn. Zo zijn kentekens als persoonsgegevens te beschouwen, evenals de combinatie van postcode en huisnummer. Ook een IP-adres kan een persoonsgegeven zijn, net als een versleuteld of gehashed persoonsgegeven. Het maakt niet uit dat je extra informatie nodig hebt (bv. het kentekenregister, of specifieke wachtwoorden om encryptie ongedaan te maken) om een gegeven te herleiden tot een persoon.

2.3.4. Verwerking van persoonsgegevens

‘Verwerking van persoonsgegevens’ omvat in principe alles wat je met een persoonsgegeven kunt doen. Dus verzamelen, opslaan, inzien, inzage erin geven, aan derden verstrekken, bewaren, et cetera. Ook het wissen of versleutelen van persoonsgegevens is een verwerking.

2.3.5. Betrokkene

De ‘betrokkene’ is degene op wie een persoonsgegeven betrekking heeft.

2.3.6. Bijzondere en gevoelige persoonsgegevens

Dit zijn persoonsgegevens die extra dienen te worden beschermd, omdat misbruik ervan een extra grote impact kan hebben op de persoonlijke levenssfeer van de betrokkene. Als dergelijke gegevens bij een datalek worden gelekt zal dit ook eerder gemeld moeten worden aan de AP, of mogelijk zelfs aan alle betrokkenen.

Voorbeelden zijn gegevens over iemands ras, godsdienst, gezondheid of seksuele leven, strafrechtelijke gegevens e.d., maar ook iemands BSN (burgerservicenummer) en andere gegevens die kunnen worden gebruikt voor identiteitsfraude. Zie verder hierna, § 3.3.1.

2.3.7. Verantwoordelijke

De ‘verwerkingsverantwoordelijke’ is degene die bepaalt dát, en hoe de verwerking van persoonsgegevens moet plaatsvinden. Of zoals de wet het zegt: degene die “het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.”

Alle verplichtingen van de AVG rusten op de verwerkingsverantwoordelijke. Die moet ervoor zorgen dat de verwerking van persoonsgegevens steeds in overeenstemming met de wet gebeurt.

2.3.8. Verwerker

Als een verwerkingsverantwoordelijke de verwerking van persoonsgegevens geheel of gedeeltelijk uitbesteedt aan een derde partij, dan is die derde partij een ‘verwerker’ in de zin van de AVG.

De inschakeling van een verwerker doet niet af aan de verplichtingen van de verwerkingsverantwoordelijke. Wel moet de verwerkingsverantwoordelijke in een speciale

verwerkersovereenkomst afspraken maken om ervoor te zorgen dat ook de verwerker de op de verwerkingsverantwoordelijke rustende verplichtingen ten aanzien van de verwerking nakomt. Tot de belangrijkste afspraken behoren die ten aanzien van de beveiliging en ten aanzien van de melding aan de verwerkingsverantwoordelijke van bij de verwerker ontstane datalekken.

3. Protocol melding datalekken

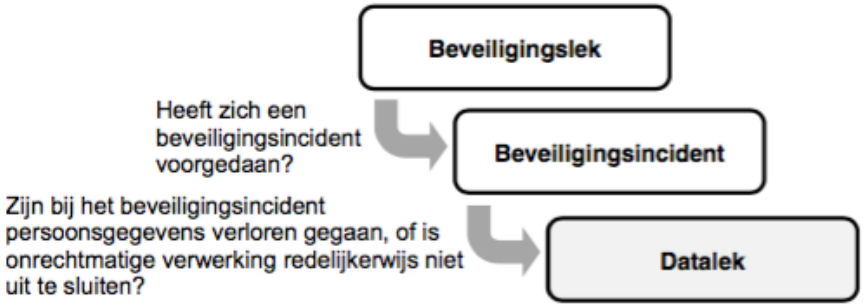
Dit hoofdstuk bevat het eigenlijke protocol. De stappen zijn: bepaal of er sprake is van een datalek (§ 3.1), neem actie (§ 3.2), melding bij de AP (§ 3.3), melding bij betrokkenen (§ 3.4) en het bijhouden van een overzicht van meldplichtige datalekken (§ 3.5). De laatste paragraaf (§ 3.6) is ter informatie; hierin wordt beschreven wat je na de melding van een datalek van de AP kunt verwachten.

3.1. Bepaal of er sprake is van een datalek

Niet elk lek is een datalek. Er is een onderscheid tussen:

a. een beveiligingslek;
b. een beveiligingsincident; en
c. een datalek.

In schema, met daarna een toelichting:[1]



3.1.1. Beveiligingslek

Van een beveiligingslek is sprake als er een zwakke plek is geconstateerd in de beveiliging. Uiteraard moet dat zo snel mogelijk worden opgelost, maar zo lang uitgesloten kan worden dat er daadwerkelijk iets fout is gegaan, hoeft dit niet aan de AP te worden gemeld. Maar uiteraard wél aan de Contactpersoon Privacy!

⇒ Een voorbeeld: iemand heeft de nieuwe inloggegevens voor z'n PC op een briefje aan het beeldscherm gevestigd. Daardoor zou elke collega van zijn account gebruik kunnen maken en onbevoegd kennis kunnen nemen van gegevens. Aan de hand van logbestanden is echter vast te stellen dat dat niet is gebeurd. Het wachtwoord moet meteen worden gewijzigd (en de desbetreffende persoon moet op zijn fout worden gewezen), maar er hoeft geen melding te worden gedaan.

3.1.2. Beveiligingsincident

Bij een beveiligingsincident zijn er daadwerkelijk gegevens verloren gegaan en/of in onbevoegde handen terecht gekomen. Zolang er echter geen persoonsgegevens bij zijn betrokken, of als redelijkerwijs kan worden uitgesloten dat als gevolg van het incident persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt is er nog geen sprake van een datalek.

[1] Gebaseerd op de hiervoor in Hoofdstuk 1 ('Vooraf') genoemde Beleidsregels van de AP (pag. 4), te vinden via https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

Dus: in elk geval melden bij de interne Contactpersoon Privacy. Als het allemaal klopt, hoeft deze geen melding te doen bij de AP.

⇒ Een voorbeeld: de systeembeheerder maakt een fout, waardoor een hele database met persoonsgegevens wordt gewist. De database is echter snel weer hersteld op basis van een actuele, complete back-up. Melden aan de AP (of betrokkenen) is niet nodig

3.1.3. Datalek

Als bij een beveiligingsincident persoonsgegevens onrechtmatig zijn verwerkt, dan is er sprake van een datalek. Hierbij geldt: bij twijfel niet inhalen. De meeste systemen bevatten persoonsgegevens en bij een incident kan je zonder nader onderzoek zelden garanderen dat die geen gevaar hebben gelopen.

Wederom: zo snel mogelijk melden bij de Contactpersoon Privacy, die hier de regie zal nemen. Er moet actie worden ondernomen om het gebleken gebrek in de beveiliging weg te nemen, om verdere schade zo veel mogelijk te beperken en om reeds ontstane schade te herstellen.

Bovendien moet zo snel mogelijk worden bepaald of het datalek ook moet worden gemeld en zo ja, wat er allemaal moet worden gemeld, en aan wie.

NB: indien een melding moet worden gedaan, moet dat binnen 72 uur na constatering van het datalek!

3.2. Acties bij constatering van een datalek

Bij constatering van een datalek zal de Contactpersoon Privacy de nodige feitelijke maatregelen moeten (doen) treffen om:

- de gebleken tekortkoming in de beveiliging te repareren (correctieve maatregelen),
- verdere nadelige gevolgen van het datalek te voorkomen of in elk geval zo veel mogelijk te beperken (repressieve maatregelen), en om
- de reeds ingetreden gevolgen zo veel mogelijk te verhelpen (herstelmaatregelen).

Daarnaast moet worden bezien of het datalek ook moet worden gemeld aan de AP, en vervolgens of dit niet óók moet worden gemeld aan de betrokkene(n) van wie de gegevens (mogelijk) verloren zijn gegaan of onrechtmatig zijn gebruikt. Deze afweging wordt gedaan door de Contactpersoon Privacy, die zich daarbij primair zal baseren op § 3.3 (over de melding aan de AP), respectievelijk § 3.4 (over de melding aan betrokkenen).

Tot slot zal de Contactpersoon Privacy een overzicht bijhouden van alle datalekken die onder de meldplicht vallen. Hierover gaat § 3.5.

3.3. Melding van het datalek aan de Autoriteit Persoonsgegevens

Een datalek hoeft alléén te worden gemeld aan de AP, als het “leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.”

Dit is hoe dan ook het geval als er gevoelige gegevens zijn gelekt. Dat wordt hieronder uitgewerkt in § 3.3.1. Daarnaast kan de meldplicht ook voortvloeien uit de verdere aard en de omvang van de inbreuk. Zie daarover § 3.3.2.

3.3.1. Zijn er gegevens van gevoelige aard gelekt?

Als door het datalek (mogelijk) persoonsgegevens van gevoelige aard zijn getroffen, moet het datalek hoe dan ook worden gemeld bij de AP.

Gegevens van gevoelige aard zijn:[2]

- 'Bijzondere' persoonsgegevens zoals bedoeld in de AVG.
  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

- Gegevens over de financiële of economische situatie van de betrokkene.
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.

- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene.
  Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.

- Gebruikersnamen, wachtwoorden en andere inloggegevens.
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- Gegevens die kunnen worden misbruikt voor (identiteits)fraude.
  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn). Ook gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen (bijvoorbeeld het medisch beroepsgeheim) vallen, moeten tot de persoonsgegevens van gevoelige aard worden gerekend.

3.3.2. Zijn de aard of de omvang van de inbreuk reden om te melden?

De aard en omvang van de getroffen verwerking zijn mede bepalend voor de beantwoording van de vraag of er bij een datalek sprake is van nadelige gevolgen voor de bescherming van persoonsgegevens, of van een aanzienlijke kans daarop. Daarbij is het volgende relevant.

Wat de omvang betreft, kan het gaan om veel gegevens per persoon, en/of om de gegevens van grote groepen personen. In het criminele circuit worden dergelijke datasets graag verhandeld, waardoor de betrokkenen daar lang last van kunnen houden.

Ook geldt dat hoe ingrijpender de beslissingen zijn die op basis van de verwerkte persoonsgegevens worden genomen, hoe groter de impact van een datalek voor de betrokkenen. Als voorbeeld kan

[2] Letterlijk overgenomen uit de hiervoor in Hoofdstuk 1 ('Vooraf') genoemde Beleidsregels van de AP (pag. 26-27) te vinden via https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken.

gedacht worden aan verloren gegane gegevens die bepalend zijn voor iemands uitkering of voor de vraag of hij een hypotheek kan krijgen.

Meer specifiek geldt voor gegevensverwerkingen door de overheid, dat er vaak sprake is van ketens van verwerkingen. Als ergens in die keten een datalek optreedt zijn de gevolgen vaak moeilijk te overzien of te corrigeren. Dat kan dus ook bij een werkgever zijn! Ook dit is een reden op grond waarvan het datalek moet worden gemeld bij de AP.

3.3.3. Wanneer, hoe en wat moet er worden gemeld aan de AP?

Een datalek moet zonder onnodige vertraging, en in elk geval binnen 72 uur na constatering worden gemeld aan de AP.

NB, als het datalek wordt geconstateerd door een verwerker (zie § 2.3.8), begint die termijn te lopen vanaf het moment van constatering door de verwerker.

Als je later dan na die 72 uur de melding doet, kan de AP vragen om een motivatie.

De melding kan het beste worden gedaan door middel van een webformulier van de AP, dat is te vinden op https://datalekken.autoriteitpersoonsgegevens.nl/.

Uit de vragen van het webformulier blijkt welke informatie over het datalek aan de AP moet worden verstrekt.[3] Als je niet alle gegevens op tijd beschikbaar hebt, kan je de melding doen met de gegevens die je wel al hebt en de melding naderhand aanvullen.

3.4. Melding aan de betrokkene(n)

In sommige gevallen moet een datalek behalve aan de AP, ook gemeld worden aan de betrokkene(n) van wie de gegevens door het datalek zijn getroffen. Dit is het geval als de inbreuk waarschijnlijk ook nog ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van die individuele betrokkene(n). Ook die kennisgeving moet zo snel mogelijk worden gedaan.

De gedachte hierachter is, dat deze betrokkene door de kennisgeving alert(er) zal zijn op de mogelijke gevolgen van het datalek, en dat hij of zij de kans heeft om eventuele voorzorgsmaatregelen te nemen (zoals het wijzigen van een wachtwoord of het blokkeren van een bankpas).

3.4.1. Wanneer en in welke gevallen moet de betrokkene worden geïnformeerd?

Het is aan de Contactpersoon Privacy (eventueel na extern advies) om te bepalen of het datalek ook aan de betrokkenen moet worden gemeld. Als dat zo is, moet ook dit zo snel mogelijk gebeuren.

Uitgangspunt is dat de betrokkenen in elk geval moet worden geïnformeerd als er persoonsgegevens van gevoelige aard zijn gelekt (zie daarover hiervoor, § 3.3.1).

Voor de rest zal deze afweging op basis van de omstandigheden van het geval moeten worden gemaakt.

Verder bestaan er ook paar situaties waarin de melding aan de betrokkene in weerwil van het voorgaande achterwege kan blijven. Kort gezegd kan dat het geval zijn als de gegevens voldoende

[3] Deze staan ook in Bijlage 1 bij de eerder genoemde Beleidsregels (pag. 51 en verder); zie https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

adequaat zijn versleuteld, of als er andere technische maatregelen zijn genomen die de kennisgeving onnodig maken (bijvoorbeeld als *remote wiping* is toegepast op een verloren of gestolen apparaat).

Ook kunnen er zwaarwegende reden zijn om de kennisgeving juist achterwege te laten. Bijvoorbeeld als gegevens zijn gelekt betreffende de verslavingszorg aan een minderjarige, van wie de ouders niet op de hoogte zijn van diens verslaving.

Deze situaties worden stuk voor stuk verder uitgewerkt in de Beleidsregels, met allerlei voorbeelden.[4] Voor ons Datalekkenprotocol voert dit te ver. Om toch een idee te geven is hierna in § 3.4.3 een schema opgenomen om hiervan toch een idee te geven.

3.4.2. Inhoud en wijze van de melding aan de betrokkene

De kennisgeving aan de betrokkene bevat in elk geval de beschrijving van de aard van de inbreuk, de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen, en de maatregelen die wij de betrokkene kunnen aanbevelen om te nemen om de negatieve gevolgen van de inbreuk te beperken.

Het beste is als alle betrokkenen persoonlijk kunnen worden geïnformeerd. Als het zou gaan om grote groepen mensen van wie wij de contactgegevens hebben, zouden wij bijvoorbeeld een e-mail kunnen sturen met daarin een korte weergave van de noodzakelijke informatie en een link naar een meer uitgebreide toelichting op een website.

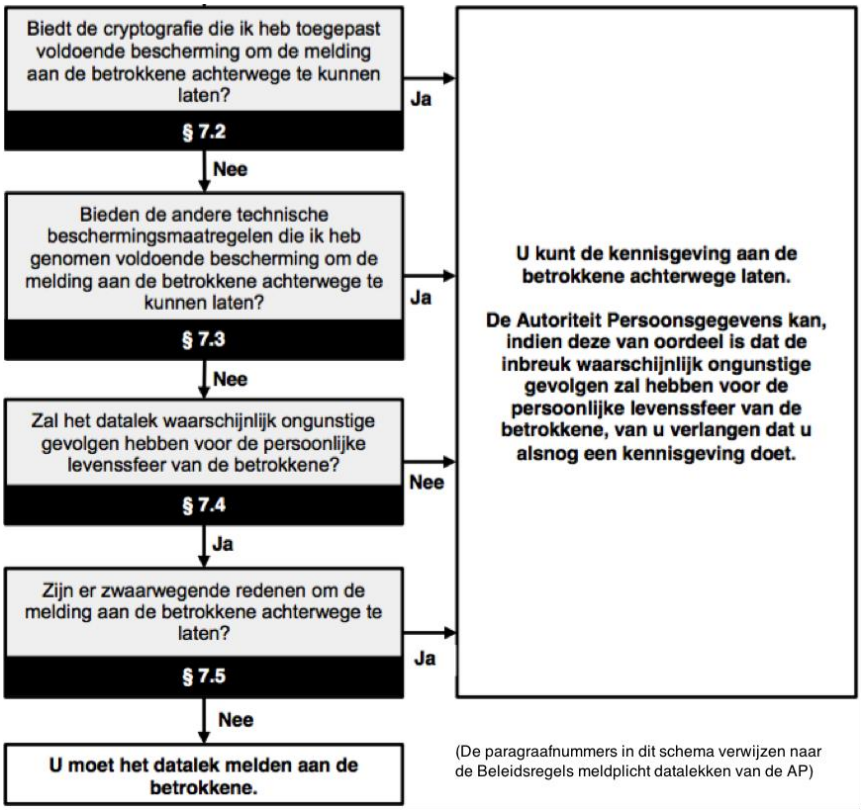
Het belangrijkste is dat zo veel mogelijk betrokkenen worden bereikt, met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken.

3.4.3. Schema: wel of niet melden aan de betrokkene

Het onderstaande schema is ontleend aan de eerder genoemde Beleidsregels. De paragraafnummers verwijzen naar de desbetreffende paragrafen daarvan.[5]

[4] Pag. 39 – 41 van de eerder genoemde Beleidsregels, zie https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

[5] De genoemde Beleidsregels, pag. 32.



3.5. Bijhouden en bewaren van een overzicht van meldplichtige datalekken

Tot slot: van alle datalekken die onder de meldplicht vallen moeten wij een overzicht bijhouden. Ook dit is een taak voor de Contactpersoon Privacy.

Dit overzicht dient een aantal doelen:[6]

- lering trekken uit het datalek en uit de wijze waarop we dit hebben afgehandeld;
- antwoord kunnen geven op vragen van betrokkenen en anderen;
- alsnog melden van het datalek aan de betrokkenen, indien wij dit in eerste instantie achterwege zouden hebben gelaten en de omstandigheden vereisen dat we dit alsnog doen.

Van elk datalek dienen de gegevens tot ten minste één jaar na de laatste melding te worden bewaard. In sommige gevallen moeten zij langer worden bewaard, bijvoorbeeld als we hebben afgezien van een kennisgeving aan de betrokkene omdat wij meenden dat onze technische beschermingsmaatregelen toereikend waren. Zoiets moet dan van tijd tot tijd worden geëvalueerd (minimaal één keer per jaar).

Wij hebben hierbij ook een eigen belang: dit overzicht is zo goed als onmisbaar ingeval er naar aanleiding van een datalek later nog eens een juridische procedure zou volgen (strafrechtelijk en/of civielrechtelijk).

[6] Beleidsregels, pag. 47.

3.6. Na de melding aan de AP

Na ontvangst van een datalekmelding stuurt de AP een ontvangstbevestiging. Ook kan de AP contact opnemen om naar aanleiding van de melding het een en ander na te vragen. Alle meldingen worden door de AP verzameld in een (niet-openbaar) register. Verder biedt de AP geen ondersteuning bij de afhandeling van het gemelde datalek.

Wel kan de AP uit een gedane melding concluderen dat ook de betrokkene geïnformeerd had moeten worden, in gevallen waarin dat nog niet is gebeurd. In zo'n geval kan de AP een aanwijzing geven - op straffe van een hoge boete - om dat alsnog te doen.

Ook kan de AP een nader onderzoek instellen als hij uit de datalekmeldingen opmaakt dat de verplichte beveiliging niet op orde is.

Als een melding achterwege is gebleven waar die wel had moeten worden gedaan, is dat een overtreding van de AVG. In dat geval kan de AP een aanwijzing geven – wederom op straffe van een hoge boete – om dat alsnog te doen, binnen een daarbij te stellen termijn.