

Protocol 'Meldplicht datalekken'

Vesac Groot Berg en Dal
Versie januari 2019

Inhoudsopgave

1. Inleiding

2. Definities

- 2.1. De Algemene Verordening Gegevensbescherming
- 2.2. Autoriteit Persoonsgegevens
- 2.3. Persoonsgegevens
- 2.4. Verwerking van persoonsgegevens
- 2.5. Verantwoordelijke voor verwerking van persoonsgegevens
- 2.6. Verwerker van persoonsgegevens
- 2.7. Betrokkene(n)
- 2.8. Datalek

3. Meldplicht datalekken

- 3.1 Is er sprake van een datalek?
- 3.2 Moet Groot Berg en Dal het datalek melden aan de Autoriteit Persoonsgegevens?
 - 3.2.1 Melding
 - 3.2.2 Verantwoordelijkheid werknemer bij melding
 - 3.2.3 Onverwijld melding
 - 3.2.4 Geen melding
- 3.3 Moet Groot Berg en Dal het datalek melden aan de betrokkene(n)?
 - 3.3.1 Melding
 - 3.3.2 Verantwoordelijkheid werknemer bij melding
 - 3.3.3 Onverwijld melding
 - 3.3.4 Geen melding

4. Vastleggen gegevens over datalek

- 4.1 Overzicht datalekken
- 4.2 Bewaartermijn

5. Sancties

- 5.1 Belang naleving meldplicht datalekken
- 5.2 Schriftelijke waarschuwing
- 5.3 Schorsing
- 5.4 Ontslag
- 5.5 Verhaal schade

6. Slotbepalingen

- 6.1 Toepassing protocol
- 6.2 Wijzigingen protocol
- 6.3 Inwerkingtreding

7. Samenvatting: wat is voor de werknemers van Groot Berg en Dal het belangrijkste om te onthouden?

- 7.1 Datalek
- 7.2 Melding datalek
- 7.3 Sancties

1. Inleiding

Op grond van de 'meldplicht datalekken' hebben bedrijven, overheden en andere organisaties die persoonsgegevens (zoals bijvoorbeeld gegevens van klanten) verwerken, de plicht om datalekken te melden aan de Autoriteit Persoonsgegevens. In sommige gevallen moet een datalek ook aan de betrokkene(n) zelf worden gemeld.

De werknemer of externe werkracht zoals omschreven in artikel 6.1 van dit protocol (hierna: werknemer) van Vesac Groot Berg en Dal (hierna: 'Groot Berg en Dal') dient ieder vermoeden van datalekken aan Groot Berg en Dal te melden. Wanneer Groot Berg en Dal zich niet aan de regels houdt, kan de Autoriteit Persoonsgegevens namelijk forse boetes aan Groot Berg en Dal opleggen. Deze boetes bedragen maximaal 20 miljoen euro per overtreding of, indien de Autoriteit Persoonsgegevens daartoe aanleiding ziet, 4% van de (wereldwijde) jaaromzet. Het is dus van groot belang dat iedere werknemer binnen Groot Berg en Dal deze meldplicht serieus neemt.

Om de regels rondom de meldplicht datalekken zo goed mogelijk te kunnen naleven, is het belangrijk dat iedereen binnen de organisatie op de hoogte is van de regels en van wat er van hem of haar wordt verwacht in het kader van de meldplicht datalekken. In dit protocol wordt omschreven hoe Groot Berg en Dal en de werknemers van Groot Berg en Dal dienen te handelen bij (een vermoeden van) datalekken.

2. Definities

2.1. Algemene Verordening Gegevensbescherming

De Algemene Verordening Gegevensbescherming (hierna: AVG) die vanaf 25 mei 2018 geldt, bevat regels over privacy en over wat er wel en niet mag gebeuren met persoonsgegevens.

2.2. Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens houdt toezicht op gebruik van persoonsgegevens door organisaties en op de naleving van de AVG.

2.3. Persoonsgegevens

Alle gegevens en informatie die herleidbaar zijn tot een persoon. Persoonsgegevens kunnen ook gegevens zijn die indirect iets over iemand zeggen.

2.4. Verwerking van persoonsgegevens

Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder (maar niet uitsluitend) het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding, terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen of vernietigen van persoonsgegevens. Denk bijvoorbeeld aan het verwerken van gegevens van bewoners in onze administratie.

2.5. Verantwoordelijke voor verwerking van persoonsgegevens

De natuurlijke persoon, rechtspersoon of het bestuursorgaan die/dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit protocol heeft te gelden dat Groot Berg en Dal als verantwoordelijke wordt aangemerkt.

2.6. Verwerker van persoonsgegevens

Degene die ten behoeve van de verantwoordelijke (Groot Berg en Dal) persoonsgegevens verwerkt.

2.7. Betrokkene(n)

Degene op wie een persoonsgegeven betrekking heeft. Binnen Groot Berg en Dal kan dit bijvoorbeeld een bewoner zijn, maar ook een werknemer of opdrachtgever.

2.8. Datalek

Bij een datalek gaat het om toegang tot of vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekkende) van gegevens, maar ook onrechtmatige verwerking van gegevens, en verlies van (toegang tot) persoonsgegevens.

2.9. Verlies of onrechtmatige verwerking

Voor de meldplicht datalekken geldt dat er sprake moet zijn van datalekken waarbij sprake is van verlies of onrechtmatige verwerking van persoonsgegevens. Daaronder wordt verstaan onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot persoonsgegevens.

2.10 *Officer Meldplicht Datalekken*

Binnen Groot Berg en Dal wordt een functionaris aangesteld die eindverantwoordelijke is voor de correcte naleving van dit protocol. Deze functie van Officer Meldplicht Datalekken wordt binnen Groot Berg en Dal bekleed door de heer Bronstijn.

3. Meldplicht datalekken

3.1. *Is er sprake van een datalek?*

Op grond van de AVG is Groot Berg en Dal verplicht om passende technische en organisatorische maatregelen te treffen om de door haar verwerkte persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige (dat wil zeggen: door iemand die daartoe niet geautoriseerd is) verwerking. Een datalek wordt gedefinieerd als een inbreuk op deze beveiliging van persoonsgegevens. Het gaat daarbij om alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment niet goed meer is en waardoor deze persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Denk aan de volgende voorbeelden:

- een kwijtgeraakte USB-stick;
- een gestolen laptop;
- een inbraak door een hacker;
- verzending van een e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
- een malware-besmetting, bijvoorbeeld door een computervirus, of;
- een calamiteit als een brand in een datacentrum waarbij gegevens verloren gaan en er geen back-up is.

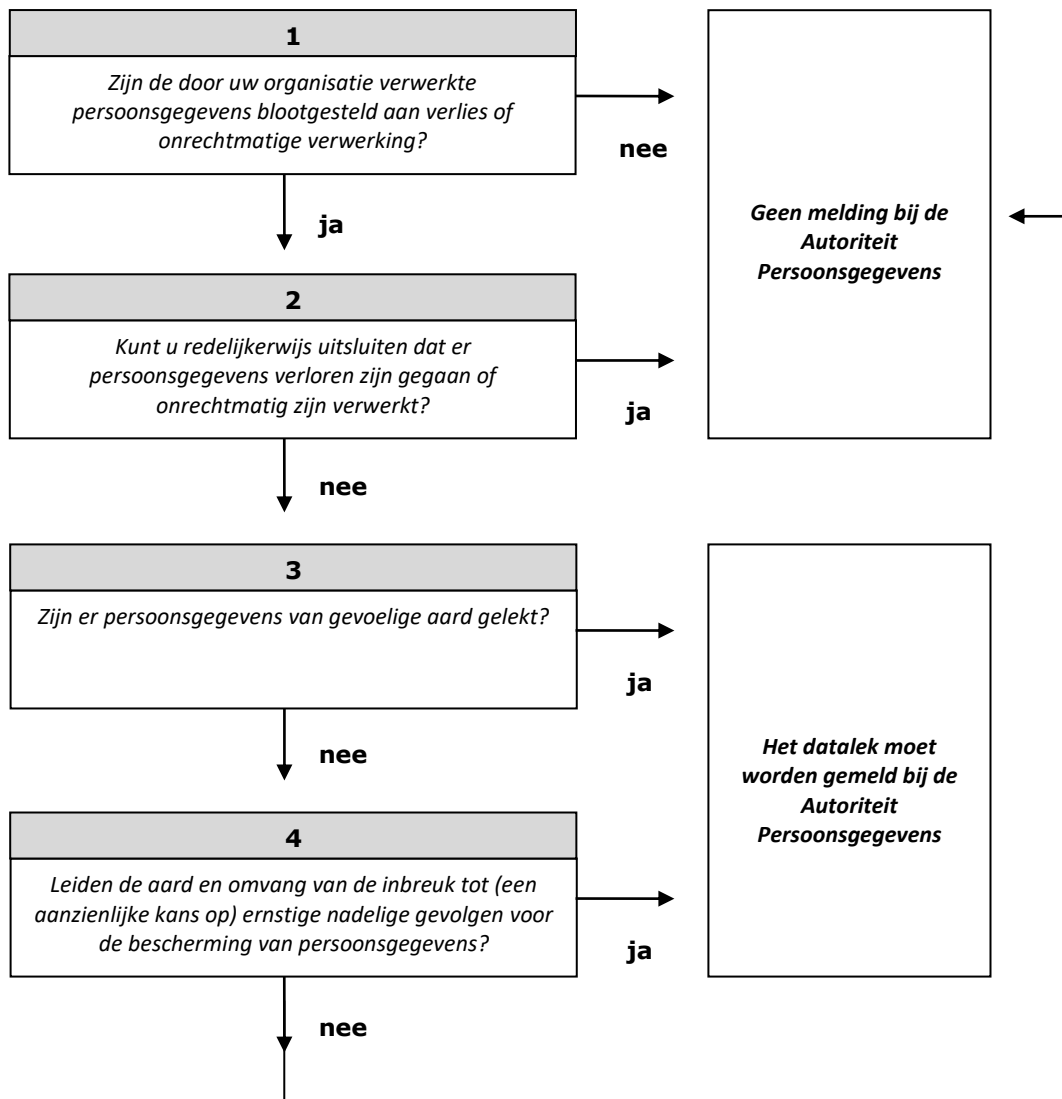
Let op: er zijn meer voorbeelden te bedenken! Ook in andere, vergelijkbare situaties waarin het mogelijk is dat persoonsgegevens verloren zijn gegaan of zijn blootgesteld aan onrechtmatige verwerking, kan er sprake zijn van een datalek.

3.2. *Moet Groot Berg en Dal het datalek melden aan de Autoriteit Persoonsgegevens?*

Niet alle datalekken hoeven aan de Autoriteit Persoonsgegevens worden gemeld. De AVG schrijft voor dat een datalek moet worden gemeld, wanneer het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het is aan Groot Berg en Dal om te bepalen of sprake is van een dergelijk datalek.

Wanneer Groot Berg en Dal ten onrechte geen melding zou doen, loopt Groot Berg en Dal het risico op forse boetes, die kunnen oplopen 20 miljoen euro per overtreding of, indien de Autoriteit Persoonsgegevens daartoe aanleiding ziet, tot 4% van de jaaromzet. Gezien de grote financiële risico's die Groot Berg en Dal loopt, zal Groot Berg en Dal bij de beoordeling van de vraag of een datalek moet worden gemeld, steeds als uitgangspunt nemen dat dit het geval is. Enkel wanneer duidelijk is dat een datalek niet hoeft te worden gemeld, laat Groot Berg en Dal een melding achterwege. In geval van enige twijfel pleegt de Officer Meldplicht Datalekken telefonisch overleg met de Autoriteit Persoonsgegevens en worden de bevindingen naar aanleiding van dit overleg schriftelijk vastgelegd.

Om te bepalen of sprake is van een datalek dat Groot Berg en Dal aan de Autoriteit Persoonsgegevens moet melden, maakt Groot Berg en Dal de volgende afweging:



Enkel wanneer bij het doorlopen van dit stroomschema, de conclusie luidt dat er geen melding van het datalek aan de Autoriteit Persoonsgegevens hoeft te worden gedaan, zal Groot Berg en Dal hier niet toe overgaan. Bij twijfel wordt dus altijd een melding gedaan!

3.2.1. Melding

Via het [Meldloket Autoriteit Persoonsgegevens](#) kan een melding worden ingediend, een bestaande melding worden aangepast of kan een bestaande melding worden ingetrokken. Dit moet gebeuren binnen 72 uur nadat het datalek is geconstateerd. Groot Berg en Dal zorgt er in elk geval voor dat de op dit webformulier gevraagde gegevens worden ingevuld en aan de Autoriteit Persoonsgegevens worden toegestuurd. Indien Groot Berg en Dal daartoe aanleiding ziet, voorziet Groot Berg en Dal de Autoriteit Persoonsgegevens eveneens van aanvullende informatie over het datalek.

3.2.2. *Verantwoordelijkheid werknemer bij melding*

De Officer Meldplicht Datalekken of een andere werknemer van Groot Berg en Dal die de melding bij de Autoriteit Persoonsgegevens doet, controleert of er een ontvangstbevestiging van de Autoriteit Persoonsgegevens is ontvangen. Zo kunnen we controleren of melding goed is ontvangen door de Autoriteit Persoonsgegevens. De kans bestaat dat de Autoriteit Persoonsgegevens de herkomst van de melding controleert. De werknemer van Groot Berg en Dal die een dergelijke vraag van de Autoriteit Persoonsgegevens ontvangt, draagt er zorg voor dat de vraag of eventuele vragen van de Autoriteit Persoonsgegevens zo spoedig mogelijk en op deugdelijke wijze worden beantwoord.

3.2.3. *Onverwijld melding*

De werknemer die het mogelijke datalek constateert, doet hiervan dezelfde werkdag nog persoonlijk melding bij de Officer Meldplicht Datalekken (zie 2.10). Wanneer dit niet mogelijk is, stuurt de werknemer de Officer Meldplicht Datalekken een e-mail over het vermeende datalek, waarna hij of zij het vermeende datalek bij de eerstvolgende gelegenheid persoonlijk aan de Officer Meldplicht Datalekken toelicht.

Op grond van de AVG, moet Groot Berg en Dal een datalek onverwijld (dat wil zeggen: zo spoedig mogelijk) aan de Autoriteit Persoonsgegevens melden. Groot Berg en Dal mag na het ontdekken van een (mogelijk) datalek, wel enige tijd nemen voor nader onderzoek, om te voorkomen dat er onnodige meldingen aan de Autoriteit Persoonsgegevens worden gedaan. Zodra duidelijk is dat sprake is van een datalek dat aan de Autoriteit Persoonsgegevens moet worden gemeld, dient Groot Berg en Dal zo spoedig mogelijk tot melding over te gaan. Het is daarom van groot belang dat de werknemers van Groot Berg en Dal snel en adequaat handelen wanneer sprake is van een (vermeend) datalek.

3.2.4. *Geen melding*

Wanneer Groot Berg en Dal tot de conclusie komt dat er geen melding aan de Autoriteit Persoonsgegevens hoeft te worden gedaan, wordt er geen melding gedaan. Groot Berg en Dal zorgt wel altijd voor een deugdelijke vastlegging van het datalek, een en ander conform het bepaalde in hoofdstuk 4 van dit protocol.

3.3. *Moet Groot Berg en Dal het datalek melden aan de betrokkene(n)?*

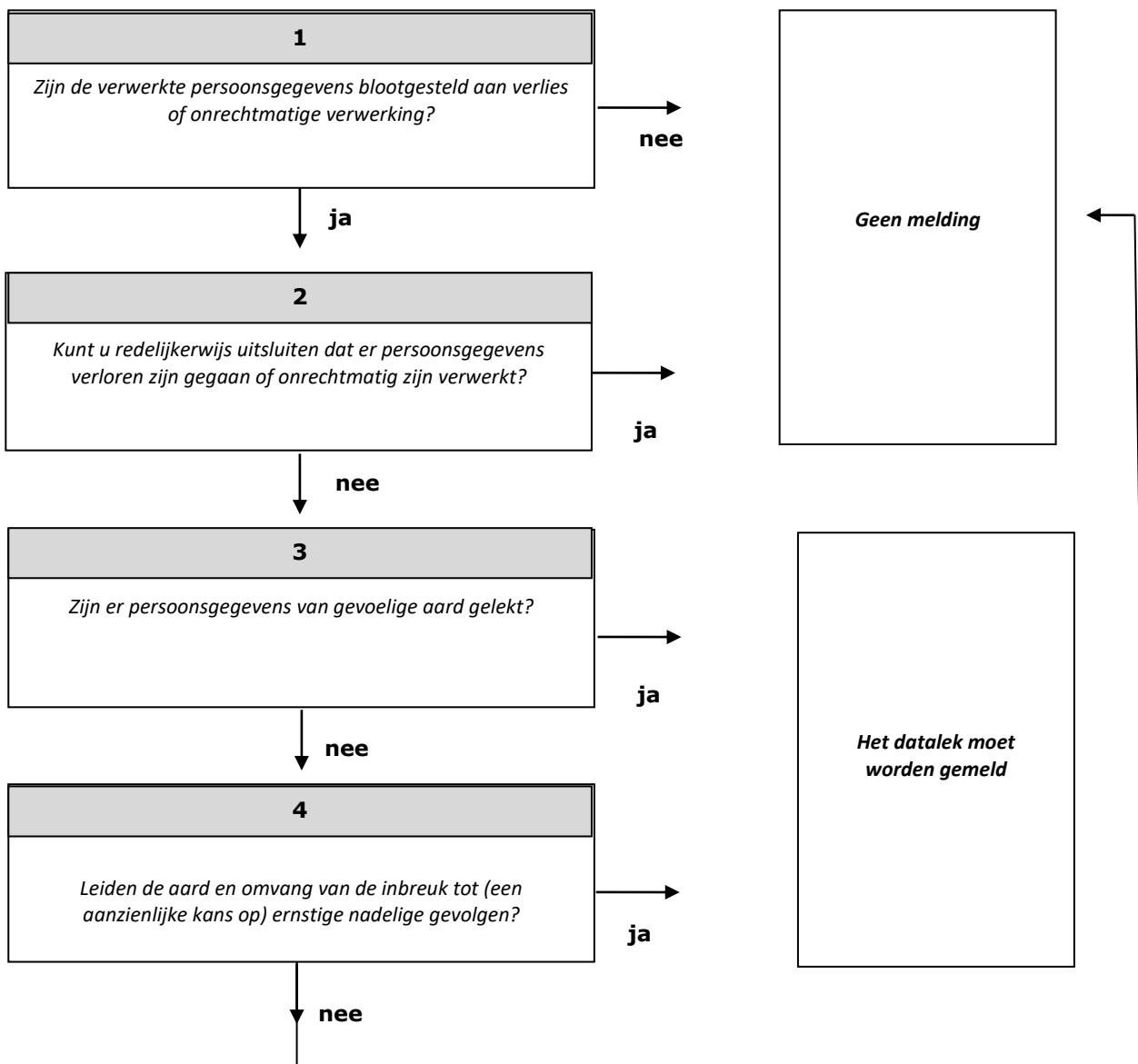
In sommige gevallen moet een datalek ook aan de betrokkene(n) worden gemeld. Dit is met name het geval wanneer een datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene(n). Een datalek hoeft enkel aan de betrokkene(n) te worden gemeld, wanneer het datalek ook aan de Autoriteit Persoonsgegevens is gemeld.

De beantwoording van de vraag of een datalek aan de betrokkene(n) moet worden gemeld, is van diverse omstandigheden afhankelijk. Zo moet worden onderzocht of de technische maatregelen (beveiliging) die Groot Berg en Dal heeft getroffen, voldoende bescherming biedt om een melding aan de betrokkene(n) achterwege te kunnen laten. De Autoriteit Persoonsgegevens controleert dit streng. De persoonsgegevens moeten worden beschermd door middel van encryptie of door *remote wiping* (waarbij gegevens die op een apparaat opgeslagen staan op afstand kunnen worden gewist). Groot Berg en Dal zal steeds van geval tot geval moeten beoordelen of de technische maatregelen voldoende bescherming bieden.

Verder moet worden onderzocht of het datalek waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n). Dit is steeds ter beoordeling van Groot Berg en Dal en moet van geval tot geval worden beoordeeld. Wanneer sprake is van persoonsgegevens van gevoelige aard, zal Groot Berg en Dal het datalek in elk geval aan de betrokkene(n) melden.

Tot slot mag Groot Berg en Dal onderzoeken of er zwaarwegende redenen zijn om een melding aan de betrokkene(n) achterwege te laten. Daarbij geldt wel dat de melding aan de betrokkene(n) alleen achterwege mag blijven als dit *noodzakelijk* is met het oog op deze zwaarwegende belangen. De Autoriteit Persoonsgegevens noemt als voorbeeld de situatie waarin een beursgenoteerde vennootschap is verwickeld in een overname wanneer zich een groot datalek voordoet. Deze onderneming zou met succes kunnen stellen dat een melding vanwege haar zwaarwegende belangen in het kader van de overname, achterwege dient te blijven. Het feit dat het doen van een melding administratieve lasten met zich brengt, vormt volgens de Autoriteit Persoonsgegevens geen zwaarwegende reden om een melding achterwege te laten.

Om te bepalen of sprake is van een datalek dat Groot Berg en Dal aan de betrokkene(n) moet melden, maakt Groot Berg en Dal de volgende afweging:



Enkel wanneer bij het doorlopen van dit stroomschema, de conclusie luidt dat er geen melding van de datalek aan de betrokkene(n) hoeft te worden gedaan, zal Groot Berg en Dal hier niet toe overgaan. Bij twijfel wordt dus altijd een melding gedaan!

3.3.1. *Melding*

Indien aan de betrokkene(n) een melding van het datalek wordt gedaan, dan moet de betrokkene(n) in elk geval in kennis worden gesteld van de aard van het datalek, de instanties waar de betrokkene(n) meer informatie over het datalek kan krijgen en de maatregelen die Groot Berg en Dal de betrokkene(n) adviseert te nemen om de negatieve gevolgen van het datalek te beperken. Groot Berg en Dal neemt in de melding tevens de contactgegevens op van de contactpersoon binnen Groot Berg en Dal met wie de betrokkene(n) contact kan opnemen indien hij of zij vragen heeft over het datalek.

3.3.2. *Verantwoordelijkheid werknemer bij melding*

De Officer Meldplicht Datalekken die een melding bij de Autoriteit Persoonsgegevens doet, onderzoekt aan de hand van dit protocol of ook een melding aan de betrokkene(n) moet worden gedaan. Bij twijfel pleegt de Officer Meldplicht Datalekken overleg met de directie. Indien aan de betrokkene(n) een melding moet worden gedaan, zorgt de daarvoor verantwoordelijke werknemer ervoor dat deze melding onverwijld aan de betrokkene(n) wordt gedaan.

3.3.3. *Onverwijld melding*

Op grond van de AVG, moet Groot Berg en Dal een datalek dat aan de Autoriteit Persoonsgegevens moet worden gemeld, onverwijld (dat wil zeggen: zo spoedig mogelijk) aan de betrokkene(n) melden, uiterlijk binnen 72 uur nadat het datalek is geconstateerd. Hoewel Groot Berg en Dal na het ontdekken van een (mogelijk) datalek, wel enige tijd mag nemen voor nader onderzoek, moet Groot Berg en Dal er rekening mee houden dat de betrokkene(n) mogelijk maatregelen moet treffen om zich te beschermen tegen mogelijke nadelige gevolgen van het datalek. Het is daarom van groot belang dat de werknemers van Groot Berg en Dal snel en adequaat handelen wanneer sprake is van een (vermeend) datalek.

3.3.4. *Geen melding*

Wanneer Groot Berg en Dal tot de conclusie komt dat geen melding aan de betrokkene(n) hoeft te worden gedaan, wordt geen melding gedaan. Wanneer door Groot Berg en Dal geen melding aan de betrokkene(n) wordt gedaan maar wel aan de Autoriteit Persoonsgegevens, dan kan de Autoriteit Persoonsgegevens op een later moment alsnog van Groot Berg en Dal verlangen dat een melding aan de betrokkene(n) wordt gedaan. In dat geval zorgt Groot Berg en Dal alsnog voor een onverwijld melding aan de betrokkene(n). In elk geval zorgt Groot Berg en Dal voor een deugdelijke vastlegging van het datalek, een en ander conform het bepaalde in hoofdstuk 4 van dit protocol.

4. Vastleggen gegevens over datalek

4.1. Overzicht datalekken

Groot Berg en Dal is op grond van de wet verplicht om een overzicht bij te houden van alle datalekken die onder de meldplicht vallen. Deze gegevens worden voor de volgende doeleinden bewaard:

- lering trekken uit het datalek en uit de wijze waarop Groot Berg en Dal dit heeft afgehandeld;
- antwoord kunnen geven op vragen van betrokkene(n) en derden;
- alsnog melden van het datalek aan de betrokkene(n), indien Groot Berg en Dal dit in eerste instantie achterwege heeft gelaten en de omstandigheden vereisen dat Groot Berg en Dal dit alsnog doet.

Voor Groot Berg en Dal is van groot belang dat zij de wettelijke regels rondom dit onderwerp, zo stipt mogelijk naleeft. Omdat Groot Berg en Dal het belangrijk vindt om lering te kunnen trekken uit eerdere (vermeende) datalekken, kiest Groot Berg en Dal ervoor om ook de gegevens over de wijze waarop de datalekken zijn ontstaan te bewaren, die niet aan de Autoriteit Persoonsgegevens moeten worden gemeld. Daarbij worden vanzelfsprekend geen persoonsgegevens bewaard wanneer daar geen wettelijke grondslag voor aanwezig is.

4.2. Bewaartermijn

De wet schrijft niet voor hoe lang Groot Berg en Dal deze gegevens moet bewaren. Om er zeker van te zijn dat gegevens over datalekken niet te vroeg worden vernietigd, hanteert Groot Berg en Dal een bewaartermijn van twee jaar.

5. Sancties

5.1. Belang naleving meldplicht datalekken

Wanneer Groot Berg en Dal de regels rondom de meldplicht datalekken niet naleeft, loopt Groot Berg en Dal het risico op forse boetes. Groot Berg en Dal heeft dan ook een groot (financieel) belang bij een correcte naleving van de regels hieromtrent door haar werknemers. In sommige gevallen kan voor Groot Berg en Dal aanleiding bestaan om sancties op te leggen, wanneer hetgeen hierover in dit protocol is bepaald, niet volledig (correct) wordt nageleefd.

In dit hoofdstuk wordt uiteengezet welke sancties Groot Berg en Dal in dat verband kan opleggen. Groot Berg en Dal behoudt zich het recht voor om ook andere sancties op te leggen op overtreding van een of meerdere bepalingen uit dit protocol. Verder is Groot Berg en Dal niet gebonden aan de hier gehanteerde volgorde bij het opleggen van sancties. Welke sanctie wordt opgelegd, is afhankelijk van de omstandigheden van het geval, waaronder de aard en omvang van de schending en de omvang van de gevolgen daarvan voor Groot Berg en Dal.

5.2. Verantwoordelijke werknemer

Indien er sprake is van een datalek kunnen meerdere werknemers betrokken zijn. Indien in dit kader de relevante bepalingen in dit protocol niet volledig (correct) worden nagekomen, wordt de exacte rol van de betrokken werknemers in samenspraak met de Officer Meldplicht Datalekken onderzocht. Op basis van dit onderzoek wordt vastgesteld welke werknemers verantwoordelijk dienen te worden gehouden en welke sanctie in dit verband gepast is.

5.3. Schriftelijke waarschuwing

Bij overtreding van het bepaalde in dit protocol, kan Groot Berg en Dal besluiten de werknemer een officiële en schriftelijke waarschuwing te geven. Een afschrift van de schriftelijke waarschuwing wordt bewaard in het personeelsdossier.

5.4. Boete

Bij overtreding van het bepaalde in dit protocol, kan Groot Berg en Dal besluiten de werknemer ten behoeve van Groot Berg en Dal een boete op te leggen van € 500,00 per overtreding en € 50,00 voor iedere dag of gedeelte van de dag dat die overtreding voortduurt. Voorafgaande ingebrekestelling en/of rechterlijke tussenkomst is niet vereist voor de opeisbaarheid van de boete. Van de leden 3 en 5 van artikel 7:650 BW wordt voor zover nodig afgeweken.

5.5. Ontslag

Bij overtreding van het bepaalde in dit protocol, kan Groot Berg en Dal tevens besluiten de werknemer (al dan niet op staande voet) te ontslaan. Groot Berg en Dal behoudt zich het recht voor om onderzoek in te stellen, alvorens tot ontslag (al dan niet op staande voet) over te gaan.

5.6. Verhaal schade

Groot Berg en Dal behoudt zich in alle gevallen het recht voor om af te zien van het innen van de in artikel 5.4 genoemde boete en in plaats daarvan van werknemer te verlangen dat hij de volledige schade vergoedt die Groot Berg en Dal lijdt als gevolg van het niet (correct) naleven van dit protocol. In alle gevallen is Groot Berg en Dal hoe dan ook bevoegd om tevens nakoming van werknemer te verlangen.

6. Slotbepalingen

6.1. *Toepassing protocol*

Dit protocol is van toepassing op alle werknemers van Groot Berg en Dal, alsmede op alle (externe) werkkrachten (waaronder tevens maar niet uitsluitend zzp'ers, gedetacheerden, uitzendkrachten, vrijwilligers etc.) die door of namens Groot Berg en Dal worden ingeschakeld en die op enigerlei wijze in aanraking komen met de verwerking van persoonsgegevens door of namens Groot Berg en Dal. Op zzp'ers en vrijwilligers zijn de arbeidsrechtelijke bepalingen echter niet van toepassing.

6.2. *Wijzigingen protocol*

Groot Berg en Dal behoudt zich het recht voor om de bepalingen in dit protocol, eenzijdig te wijzigen.

6.3. *Inwerkingtreding*

Dit protocol treedt in werking op 1 januari 2019.

7. Samenvatting: wat is voor de werknemers van Groot Berg en Dal het belangrijkste om te onthouden?

7.1 Datalek

Wat is een datalek? Er is sprake van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsprobleem. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een gestolen geprinte klantenlijst evengoed een datalek vormen. Andere voorbeelden zijn: cyberaanvallen, een e-mail die verzonden is naar verkeerde adressen, verzending van een e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren usb-sticks. Als een bedrijfstelefoon verloren is of gestolen wordt, dan is dat mogelijk een datalek.

Let op: er zijn meer voorbeelden te bedenken! Ook in andere, vergelijkbare situaties waarin het mogelijk is dat persoonsgegevens verloren zijn gegaan of zijn blootgesteld aan onrechtmatige verwerking, kan sprake zijn van een datalek. Twijfel je of het een datalek is, overleg dan met de Officer Meldplicht Datalekken, de heer Bronstijn.

7.2 Melding datalek door werknemer

Constaateer je een mogelijk datalek, dan moet je dit dezelfde dag nog persoonlijk melden (bijvoorbeeld door te bellen) bij de Officer Meldplicht Datalekken. Wanneer dit niet mogelijk is, stuur je de Officer Meldplicht Datalekken dezelfde dag nog een e-mail over het vermeende datalek. Zodra je wel contact kunt opnemen met de Officer Meldplicht Datalekken, meld je het vermeende datalek nogmaals persoonlijk bij hem of haar.

7.3 Sancties werknemer

Leef je het protocol niet goed na, bijvoorbeeld omdat je niet tijdig het datalek meldt, dan kan Groot Berg en Dal jou een sanctie opleggen. Voorbeelden van sancties zijn:

- een officiële en schriftelijke waarschuwing die in je personeelsdossier bewaard wordt;
- het geven van een boete van € 500,00 per overtreding en € 50,00 voor iedere dag of gedeelte van de dag dat die overtreding voortduurt. Voorafgaande ingebrekestelling en/of rechterlijke tussenkomst is niet vereist voor de opeisbaarheid van de boete. Van de leden 3 en 5 van artikel 7:650 BW wordt voor zover nodig afgeweken;
- ontslag (al dan niet op staande voet);
- in plaats van het innen van de boete, het verhalen van de volledige schade die Groot Berg en Dal lijdt door overtreding van het protocol.