Procedure Melden van datalekken Streekarchief Midden-Holland

Wanneer persoonsgegevens als gevolg van een informatiebeveiligingsincident toegankelijk worden voor mensen die geen recht hebben op kennisname van deze informatie, is sprake van een datalek. De Algemene Verordening Gegevensbescherming (AVG – van kracht met ingang van 25 mei 2018) schrijft voor dat ernstige datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens (AP). In bepaalde gevallen moet het datalek ook gemeld worden aan de 'betrokkene(n)' (de persoon /personen van wie de data zijn gelekt). Bij het niet nakomen van de meldplicht kan de Autoriteit Persoonsgegevens een boete opleggen, die hoog op kan lopen.

Hieronder volgt een omschrijving van de procedure die Streekarchief Midden-Holland (SAMH) hanteert voor de melding van datalekken.

Taken, verantwoordelijkheden en bevoegdheden

1. Binnen het SAMH is de Functionaris Gegevensbescherming (FG) verantwoordelijk voor de melding van een datalek aan de AP;
2. De Functie van FG valt binnen het SAMH samen met de functie van Hoofd Beheer;
3. Iedere medewerker die direct of indirect kennis draagt of krijgt van een datalek, is verplicht dit direct te melden aan de FG;
4. De FG beoordeelt of de ernst van het datalek aanleiding is om de AP in te lichten;
5. De FG is verantwoordelijk voor het onderzoeken van het beveiligingsincident;
6. Onder verantwoordelijkheid van de FG wordt ook bepaald wie de betrokkene gaat inlichten over een datalek;
7. De FG draagt zorg voor het documenteren van alle datalekken in een datalekkenregister;
8. Het hoofd Dienstverlening is verantwoordelijk voor het nemen van passende technische en organisatorische maatregelen;
9. De directeur is verantwoordelijk voor de actualiteit van deze procedure.

Procedure in hoofdlijnen

1. De medewerker die direct of indirect kennis draagt of krijgt van een beveiligingsincident waarbij sprake is van een inbreuk op de beveiliging van persoonsgegevens, meldt dit direct aan de FG;
2. De FG beoordeelt de ernst van het beveiligingsincident en meldt het datalek binnen 72 uur na ontdekking bij de AP;
3. Indien sprake is van een hoog risico voor de betrokkene, draagt de FG zorg voor inlichting van de betrokkene(n);
4. De FG onderzoekt het datalek. Hierbij is aandacht voor de volgende aspecten:

   a. De aard van het datalek;
   b. De oorzaak van het datalek;
   c. Beoordeling of er sprake is van het niet nakomen of een tekortkoming in de beveiligingsprocedures;
5. De FG voorziet de AP zo spoedig mogelijk van aanvullende informatie naar aanleiding van dit onderzoek;
6. Het data lek wordt gedocumenteerd en in een register vastgelegd;
7. Bij een serieus datalek informeert de FG direct het DB;
8. De deelnemende gemeente(n) wordt / worden geïnformeerd indien het datalek verband houdt met het archief van (een van) de deelnemer(s).

Interne controle

1. De geregistreerde datalekken worden jaarlijks door de FG geanalyseerd. Op basis van deze analyse stelt de FG een verbeterplan of – advies op, dat wordt opgenomen in de jaarlijkse managementrapportage en het jaarverslag.
2. Minimaal jaarlijks beoordeelt de FG of de procedure voor het melden van datalekken en uitvoering daarvan nog met elkaar in overeenstemming zijn.
3. Indien nodig, wordt de procedure geactualiseerd en worden de medewerkers nader geïnstrueerd.

Toelichting

1. Persoonsgegevens

De meldplicht datalekken is alleen van toepassing als er sprake is van de verwerking van persoonsgegevens. Dit kunnen persoonsgegevens zijn van medewerkers, bezoekers en andere betrokkenen bij het SAMH.

De AVG hanteert een ruime omschrijving voor het begrip persoonsgegevens. Het gaat om: *"alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon..." (art 4 lid 1 AVG).* Als gevolg van technologische ontwikkelingen is ook het begrip 'bijzondere persoonsgegevens' verder uitgebreid ten opzichte van de huidige Wet Bescherming persoonsgegevens.

Daarnaast wordt in de AVG de verwerking van persoonsgegevens uitvoerig omschreven: *"… het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens".*
(art. 4 lid 2 AVG)

Persoonsgegevens van overleden personen vallen niet onder de reikwijdte van de AVG.

2. Wat is een datalek?

Een data lek is een inbreuk in verband met deze persoonsgegevens, hetgeen in de AVG wordt gedefinieerd als: *'een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens'*
(artikel 4, lid 12 AVG).

Bij een datalek is er altijd sprake van een beveiligingsincident. Dit kan zijn:

- Een inbraak door een hacker
- Een gestolen of verloren laptop of usb-stick
- Een afgesloten website die open staat
- Verkeerd databeheer
- Email adressen blootgeven bij verzending naar meerdere adressen
- Onbeveiligde emails met privacygevoelige informatie
- Het verlies van gegevens bij een calamiteit (bijv. een brand)

Er moet zich echt een beveiligingsincident hebben voorgedaan, niet slechts een dreiging. Boze opzet of verwijtbaarheid is in dit verband niet relevant.

3. Meldplicht

De inbreuk in verband met persoonsgegevens moet door de FG gemeld worden aan de AP, tenzij het onwaarschijnlijk is dat het incident een risico inhoudt voor de rechten en vrijheden van de betrokkenen (artikel 33 lid 1 AVG).

Er zal moeten worden gekeken naar de aard van de getroffen gegevens. Zijn deze van gevoelige aard, dan kan er sprake zijn van een risico. Voorbeelden hiervan zijn: inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen, of gegevens over godsdienst, ras, politieke gezindheid.

4. Meldplicht aan de betrokkene

Er is tevens een mededelingsplicht aan de betrokkene wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een ***hoog*** risico inhoudt voor de rechten en vrijheden van natuurlijke personen (art 34 lid 1 AVG).

De gevoeligheid van de gegevens en kans op nadelige gevolgen moet worden meegenomen in de afweging of er sprake is van een hoog risico. Reputatieschade, discriminatie en identiteitsfraude zijn voorbeelden van nadelige gevolgen. De aard en de omvang van de inbreuk kunnen de kans op nadelige gevolgen nog verder vergroten. Beveiligingslekken bij omvangrijke verwerkingen zoals bij persoonsgegevens die binnen ketens worden gedeeld, kunnen zich als een olievlek verspreiden en ernstig nadelige gevolgen hebben.

Wanneer melding aan betrokkene nog niet heeft plaatsgevonden, kan de AP alsnog daartoe verplichten (artikel 34 lid 4 AVG).

Er is géén meldingsplicht aan de betrokkene indien:

- Passende technische en organisatorische maatregelen zijn genomen, zoals bijvoorbeeld versleuteling van gegevens (art 34 lid 3a AVG).
- Achteraf maatregelen zijn genomen waarmee de vastgestelde risico's zijn weggenomen (artikel 34 lid 3b AVG).
- Mededeling aan betrokkene onevenredig veel inspanning zou kosten. In dat geval volstaat een openbare mededeling (artikel 34 lid 3 c AVG).
- Achterwege laten van de melding noodzakelijk is ter waarborging van o.a.
  - De nationale veiligheid
  - De landsverdediging
  - De openbare veiligheid

(art 23 AVG en art 41 UAVG)

5. Registratie

Elk datalek of een vermoeden daarvan dient gedocumenteerd te worden, met inbegrip van alle feiten omtrent de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen (artikel 33 lid 5 AVG).

6. Boete

Bij het niet-nakomen van de meldplicht kan de AP een geldboete opleggen. Deze boete bedraagt max 10.000.0000 euro (artikel 58 en artikel 83 lid 4a AVG).

7. Verwerkingsverantwoordelijke en verwerker

De directie van het SAMH kan als *verwerkingsverantwoordelijke* de verwerking van persoonsgegevens uitbesteden aan een derde partij, de *verwerker*. Indien een datalek ontstaat bij de verwerker, dan zal deze het SAMH zonder onredelijke vertraging informeren, zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens (artikel 33 lid 2 AVG).

De afspraken tussen het SAMH en externe partijen worden vastgelegd in een verwerkingsovereenkomst (artikel 28 lid 3 AVG). Hierin moet onder andere worden vastgelegd op welke wijze SAMH door de verwerker op de hoogte wordt gesteld van een datalek. Het SAMH blijft als eindverantwoordelijke verantwoordelijk voor de melding van een datalek aan de AP.

Meer over de procedure

Hoe en wanneer melden?

Onder verantwoordelijkheid van de FG wordt een datalek binnen 72 uur na ontdekking gemeld aan de AP via het meldpunt datalekken:

https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Informatie die op dat moment nog ontbreekt moet zonder onredelijke vertraging verder in fasen worden aangeleverd (artikel 33 lid 4 AVG).

Als er vertraging is in het aanleveren van aanvullende informatie, dan moet deze vertraging verklaard worden (art 33 lid 1 AVG).

Indien de FG heeft beoordeeld dat het risico voor betrokkene(n) hoog is, dan zal de FG ervoor zorgdragen dat betrokkene(n) **onverwijld** geïnformeerd wordt/worden, dat wil zeggen: zo snel mogelijk nadat onderzoek heeft plaatsgevonden (artikel 34 lid 1 AVG).

De betrokkene moet in staat gesteld worden om de schade zo veel mogelijk te beperken.

Wat moet er gemeld worden aan de Autoriteit Persoonsgegevens? (artikel 33 lid 3 AVG)

De FG van het SAMH informeert de AP tenminste over:

- De aard en omvang van de inbreuk. Een samenvatting van het incident, het tijdstip en het type persoonsgegevens zijn daarbij ook van belang;
- (Waar mogelijk) vermelding van categorieën van betrokkenen, persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en hun persoonsgegevensregisters in kwestie;
- De naam en contactgegevens van de Functionaris Gegevensbescherming (of een ander contactpunt waar meer info kan worden verkregen);
- De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- De voorgestelde maatregelen om de inbreuk aan te pakken (waaronder maatregelen ter beperking van nadelige gevolgen);
- Of het SAMH de betrokkene(n) ook heeft geïnformeerd of gaat informeren over het datalek;
- De inhoud van de melding aan de betrokkenen of de reden waarom het SAMH afziet van het melden van het datalek aan de betrokkenen.

Wat moet er gemeld worden aan betrokkenen? (artikel 34 lid 2 AVG)

Onder verantwoordelijkheid van de FG wordt de betrokkene in duidelijke en eenvoudige taal geïnformeerd over:

- De aard en omvang van de inbreuk. Een samenvatting van het incident, het tijdstip en het type persoonsgegevens zijn daarbij ook van belang;
- De naam en contactgegevens van de FG (of een ander contactpunt waar meer info kan worden verkregen);
- De waarschijnlijke gevolgen van de inbreuk voor betrokkenen;

- De voorgestelde maatregelen om de inbreuk aan te pakken (waaronder maatregelen ter beperking van nadelige gevolgen) en wat de betrokkene zelf kan doen om de negatieve gevolgen te beperken.

De AP houdt een register bij van alle datalekmeldingen. Dit register wordt niet openbaar gemaakt, maar als de AP een boete oplegt, wordt dit besluit wel openbaar gemaakt. Tevens volgt openbaarmaking op het moment dat de betrokkenen worden geïnformeerd over het datalek.