Datalekprotocol Regionaal Historisch Centrum Vecht en Venen

Wat is een datalek?
Een datalek is een 'inbreuk in verband met persoonsgegevens'. Je kunt denken aan onbedoelde of ongeoorloofde toegang tot persoonsgegevens, het ongeautoriseerd vernietigen of wijzigen van persoonsgegevens of technische problemen waardoor er geen toegang is tot persoonsgegevens.

Wat moet ik doen als ik vermoed dat er een datalek is?
Neem meteen telefonisch contact op met de directeur (Roosmarijn) en indien ze onbereikbaar is neemt contact op met adviseur digitale archieven. Ze zullen het dan samen met de FG oppakken.
Bij het melden ervan wordt je tenminste gevraagd welke en welke soort gegevens er gelekt zijn, wanneer het is ontstaan (indien je dit weet), hoe je het datalek hebt ontdekt en of onbevoegden vanwege het lek toegang hadden tot de gegevens.

Aan wie kun je vragen stellen over mogelijke datalekken en de bescherming van persoonsgegevens?
Intern kunnen vragen worden gesteld aan de directeur of aan de ADA. Zij nemen contact op met de betrokken FG('s).

Inleiding
Aanleiding
Onder de Algemene Verordening Gegevensbescherming (AVG) geldt er een meldplicht voor datalekken. Deze meldplicht houdt in dat het Regionaal Historisch Centrum Vecht en Venen (RHCVV) onmiddellijk een melding moet doen bij de Autoriteit Persoonsgegevens (AP) indien er een ernstig datalek is. Soms moet het datalek ook gemeld worden aan personen van wie de persoonsgegevens zijn gelekt. Als blijkt dat niet of onvoldoende is voldaan aan deze meldplicht kan de toezichthouder een bindende aanwijzing opleggen. Dit kan uiteindelijk resulteren in een bestuurlijke boete.

Naast een datalek kan een gemeente te maken krijgen met beveiligingsincidenten. De Baseline Informatiebeveiliging Overheid (BIO) verplicht de overheid om beveiligingsincidenten te registreren, zodat er inzicht in deze incidenten komt en zodat ervan geleerd wordt. Het is niet verplicht om beveiligingsincidenten te melden bij de AP.

Dit document voorziet in de procedure tot melding en registratie van datalekken en beveiligingsincidenten.

Wat is een datalek?
Volgens de AVG is er sprake van een datalek als zich een inbreuk voordoet in verband met persoonsgegevens die verwerkt zijn. Voorbeelden van datalekken zijn:

- het verlies van een mobiel apparaat (laptop, telefoon, tablet of usb-stick) waarop gevoelige persoonsgegevens staan;
- een computer hack;
- besmetting met ransomware;
- het technisch falen van apparatuur;
- een brief, pakketje of email naar verkeerde ontvanger; persoonsgegevens bij het oud papier;
- een onherstelbaar defect apparaat (geen back-up)
- (eventueel daaruit volgend:) het onbedoeld persoonsgegevens op de website plaatsen.

Een datalek dient uiterlijk binnen 72 uur na ontdekking ervan te worden gemeld aan de AP. Indien dit later gebeurt, dan dient de melding voorzien te worden van uitleg omtrent de vertraging. Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

Niet ieder datalekincident valt onder de meldplicht. Er is sprake van een geclausuleerde meldplicht voor datalekken. Hiervoor is het noodzakelijk dat een juridische beoordeling wordt gemaakt. Artikel 33 van de AVG stelt dat een datalek gemeld dient te worden indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. In de beleidsregels van de AP staat dat een datalek alleen gemeld moet worden wanneer een aanzienlijk risico is op schade aan de persoonlijke levenssfeer van een individu. Als bijvoorbeeld verloren of

gestolen persoonsgegevens goed versleuteld zijn opgeslagen dan is er geen aanzienlijk risico op schade aan de persoonlijke levenssfeer.

Wat is een beveiligingsincident?
Het gaat om situaties waarbij de informatieveiligheid van het RHCVV in het geding is. Dit hoeft niet *direct* een relatie te hebben met persoonsgegevens. De informatieveiligheid is in het geding wanneer werkprocessen langdurig stil komen te liggen of serieuze schade ontstaat of kan ontstaan door globaal drie redenen:

- Als informatie niet beschikbaar is: bijvoorbeeld als een informatiesysteem/applicatie is uitgevallen of zeer traag is waardoor werk niet kan worden uitgevoerd;
- Als informatie niet betrouwbaar is: bijv. wanneer informatie in een systeem niet overeenkomt met de werkelijkheid, koppelingen met andere systemen niet werken etc.;
- Als personen bij informatie kunnen die hiertoe niet bevoegd zijn.

Procedure meldplicht datalekken en beveiligingsincidenten.

Deze procedure beschrijft de wijze waarop binnen het RHCVV wordt omgegaan met de meldplicht datalekken in de zin van de AVG en de registratie van beveiligingsincidenten ingevolge de BIO. Het bevat afwegingskaders bij een vermoeden van een datalek en specificeert de nodige acties.

In de procedure worden de volgende stappen onderscheiden:

1. het signaleren/intern melden van incidenten en datalekken waarbij persoonsgegevens betrokken zijn;
2. het beoordelen of het incident aangemerkt kan worden als een datalek op grond van de AVG en de richtsnoeren van de AP;
3. het beoordelen of er sprake is van een datalek dat gemeld moet worden bij de AP en betrokkene(n);
4. het nemen van (beschermings)maatregelen om het datalek of incident te dichten of verdere inbreuk te voorkomen;
5. het documenteren van het datalek of incident bij zowel interne als externe meldingen;
6. het informeren van de FG's door de ADA en van het Algemeen Bestuur en gemeentesecretarissen door de directeur
7. het melden van het datalek bij de AP

Hieronder volgt een nadere uitwerking van deze procedure.

Het signaleren/melden van beveiligingsincidenten en datalekken

Meldingen van RHCVV medewerkers

Wanneer een medewerker direct of indirect kennis draagt of krijgt van een beveiligingsincident, is deze verplicht dit direct te melden aan de directeur. Bij afwezigheid wordt het gemeld aan de ADA.

Dan worden de volgende stappen doorlopen:

1. De directeur neemt zo snel mogelijk contact op met ADA, de FG van het RHCVV en de FG's van de gemeenten.

2. Er wordt dan door de directeur, de FG en ADA van het RHCVV, met mogelijke ondersteuning vanuit de gemeenten indien het gegevens van hen betreft, onderzocht. Wanneer het interne systeem van het RHCVV betrokken is, wordt Avance gecontacteerd. Hetzelfde geldt voor DE REE bij betrokkenheid van MAIS. Hierbij is er aandacht voor de volgende aspecten:
    a. wat is de aard van het beveiligingsincident;
    b. wat is de oorzaak van het beveiligingsincident;
    c. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
    d. is er sprake van verwijtbaar handelen en door wie.

3. De ADA maakt van het beveiligingsincident een verslag. Het verslag bevat in ieder geval de volgende informatie:
   a. plaats in het RHCVV waar het beveiligingsincident zich heeft voorgedaan;
   b. op welk informatiesysteem of persoonsgegevensverwerkend proces het beveiligingsincident betrekking heeft;
   c. een beschrijving van het beveiligingsincident;
   d. opgave van de categorieën van personen waarvan de (bijzondere) persoonsgegevens betrokken zijn in het beveiligingsincident;
   e. inzicht in de getroffen maatregelen die genomen zijn om eventuele gevolgen te beperken;
   f. inzicht in de getroffen maatregelen om dergelijke beveiligingsincidenten in de toekomst te voorkomen.

4. Het team (vanuit het RHCVV de directeur, de FG en ADA en vanuit de gemeenten de FG's) beoordelen of het beveiligingsincident ernstige nadelige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n) en adviseert management en bestuur over het doen van de meldingen aan de AP en aan de betrokkene(n).

5. De directeur van het RHCVV besluit over het al dan niet doen van een melding. Deze beslissing wordt binnen 72 uur van de melding van de medewerker gemaakt.

6. De directeur doet namens het RHCVV de melding aan de AP en, indien nodig, aan de betrokkene(n). De melding aan de AP wordt binnen 72 uur van de melding van de medewerker gemaakt, indien dit langer duurt moet het RHCVV dit toelichten.

7. De directeur is aanspreekpunt voor de AP en voorziet de AP voor zover noodzakelijk van nadere toelichting.

8. Eventuele aanwijzingen van de AP worden vastgelegd en opgevolgd.

9. De ADA legt een dossier aan van het beveiligingsincident en registreert dit in de datalek- en beveiligingsincidentregister.

10. De FG informeert de Informatiebeveiligingsdienst (IBD) van de Vereniging van Nederlandse Gemeenten (VNG) en VNG-Realisatie over incidenten die gevolgen kunnen hebben voor andere verantwoordelijken.

Meldingen verwerkers
Het RHCVV laat bepaalde verwerkingen van persoonsgegevens geheel of gedeeltelijk uitvoeren door zogeheten verwerkers. Ondanks dat het RHCVV deze gegevens "buitenshuis" plaatst, is en blijft het RHCVV verantwoordelijk voor deze verwerkingen. De AVG verplicht het RHCVV namelijk om ervoor te zorgen dat de verwerking van persoonsgegevens voldoende beveiligd is, ook als bij de verwerking een verwerker is ingeschakeld.
Dit geldt ook voor de meldplicht datalekken. We moeten ervoor zorgen dat de verwerker maatregelen treft die nodig zijn zodat het RHCVV aan deze meldplicht kan voldoen.
Met de verwerkers van het RHCVV wordt in verwerkersovereenkomsten afgesproken dat de verwerkers een incident/datalek direct na constatering melden bij het RHCVV. De melding bij de AP gebeurt door de directeur van het RHCVV.
Bij een melding door een verwerker worden eveneens de stappen 1 tot en met 9 gevolgd die vermeld staan onder Meldingen van RHCVV medewerkers.

Externe signalen/meldingen.
Een incident of datalek kan ook gesignaleerd/geconstateerd worden door een derde. Denk hier bijvoorbeeld aan een websitebezoeker die persoonsgegevens vindt of iemand die van het RHCVV een mail krijgt met persoonsgegevens die niet voor die persoon bestemd zijn.
Burgers en ambtenaren kunnen een melding maken bij het RHCVV via de normale kanalen (brief, telefoon, loket, e-mail). Op onze website wordt dit op onze pagina over het privacybeleid gecommuniceerd.

Ook bij externe signalen/meldingen worden de stappen 1 tot en met 9 gevolgd die vermeld staan onder Meldingen van RHCVV medewerkers.

Het registreren van signalen/meldingen
Zoals eerder aangegeven zullen alle gemelde incidenten geregistreerd worden. De ADA neemt deze registraties op in een register. In het register is onderscheid gemaakt tussen datalekken en de registratie van beveiligingsincidenten. De ADA draagt zorg voor het beheer van dit register en informeert het bestuur jaarlijks hierover.

Het nemen van (beschermings)maatregelen.
Na het signaleren/ontdekken van een datalek/incident worden, indien mogelijk, direct passende technische en/of organisatorische beschermingsmaatregelen genomen. De FG, de ADA en Avance (het bedrijf achter de IT-infrastructuur van het RHCVV) analyseren de situatie en bekijken samen welke beschermingsmaatregelen genomen moeten worden om verdere inbreuk te voorkomen. In geval van beveiligingsincidenten kan hierover contact worden opgenomen met de Informatiebeveiligingsdienst (IBD) van de VNG voor ondersteuning en advies. Hierbij kan gedacht worden aan bijvoorbeeld:

- het verwijderen van de persoonsgegevens (bijv. op afstand bij verloren mobiele apparaten);
- het aanpassen van de toegang tot de persoonsgegevens (autorisaties);
- het terugplaatsen van een back-up.

Het nemen van beschermingsmaatregelen staat los van het feit of een datalek gemeld wordt bij de AP of de betrokkene(n) en of een incident geregistreerd moet worden. Deze maatregelen moeten namelijk sowieso genomen worden om verdere inbreuk te voorkomen.

Het register datalekken en beveiligingsincidenten.

Alle meldingen van datalekken (ook de meldingen die niet aan de AP worden gemeld) en incidenten worden geregistreerd. De ADA beheert het register.

Taken en verantwoordelijkheden met betrekking tot het melden van datalekken en beveiligingsincidenten.

1. De directeur zorgt ervoor dat het thema 'melding datalekken' voldoende aandacht krijgt, bijvoorbeeld in het werkoverleg of de terugkoppelingen van incidenten/datalekken.

2. De ADA is verantwoordelijk voor de actualiteit van deze procedure, de bekendmaking en het in kennis stellen c.q. instrueren van de medewerkers;

3. Iedere medewerker die direct of indirect kennis draagt of krijgt van een beveiligingsincident, is verplicht dit direct te melden aan de directeur;

4. De ADA is verantwoordelijk voor onderzoek en rapportage naar aanleiding van beveiligingsincident en betrekt hierbij de directeur en FG. Indien nodig worden ook IT leveranciers betrokken (Avance en DE REE).

5. De directeur verleent alle medewerking aan het onderzoek en is verantwoordelijk voor het ondernemen van preventieve en repressieve beveiligingsacties;

6. De directeur van het RHCVV is de aangewezen contactpersoon voor de AP en daarmee verantwoordelijk voor:
    - de melding aan de AP en aan betrokkenen;
    - de communicatie met de AP en betrokkenen naar aanleiding van de meldingen.

Communicatie

Bij datalekken of incidenten met een behoorlijke impact wordt de communicatie-medewerker van het RHCVV betrokken en wordt er ondersteuning gevraagd van de centrumgemeente.