PROCEDURE MELDPLICHT DATALEKKEN EN BEVEILIGINGSINCIDENTEN GEMEENTE VALKENBURG AAN DE GEUL

Hoofdstuk 1. Inleiding.

1.1. Aanleiding.

Sinds begin 2016 geldt in Nederland de meldplicht voor datalekken. Onder de Algemene verordening gegevensbescherming (AVG), die in werking is getreden op 25 mei 2018, is de meldplicht voor datalekken gehandhaafd. Deze meldplicht houdt in dat gemeenten onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. Soms moet het datalek ook gemeld worden aan de burgers 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. Ingevolge de Baseline Informatiebeveiliging Gemeente (BIG) zijn gemeenten verplicht om beveiligingsincidenten te registreren, zodat inzicht verkregen wordt in het aantal en soort en ervan geleerd wordt. Melding bij de AP van beveiligingsincidenten is niet verplicht.
Dit document voorziet in de procedure tot melding en registratie van datalekken en beveiligingsincidenten.

1.2 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).

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 aanzienlijke risico op schade aan de persoonlijke levenssfeer.

1.3 Wat is een beveiligingsincident?

Het gaat om situaties waarbij de informatieveiligheid van de gemeente in geding is. Dit hoeft niet *direct* een relatie te hebben met persoonsgegevens. De informatieveiligheid is in het geding wanneer werkprocessen langduriger stil komen te liggen of serieuze schade ontstaat of kan ontstaan door globaal 3 redenen:

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

Hoofdstuk 2 Procedure meldplicht datalekken en beveiligingsincidenten.

Deze procedure beschrijft de wijze waarop binnen de gemeente Valkenburg aan de Geul wordt omgegaan met de meldplicht datalekken in de zin van de AVG en de registratie van beveiligingsincidenten ingevolge de BIG. 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/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 portefeuillehouder en de gemeentesecretaris.

Hieronder volgt een nadere uitwerking van deze procedure.

2.1 Het signaleren/melden van beveiligingsincidenten en datalekken.

2.1.1 Meldingen van medewerkers van de gemeente Valkenburg aan de Geul.
Wanneer een medewerker van de gemeente direct of indirect kennis draagt of krijgt van een beveiligingsincident, is deze verplicht dit direct te melden aan zijn/haar direct leidinggevende en de concernjurist.

Dan worden de volgende stappen doorlopen:
1. De concernjurist en zo nodig de beveiligingsbeheerder van het specifieke vakgebied, onderzoeken het beveiligingsincident en betrekken hierbij de direct leidinggevende en de privacy en security officer. Hierbij is aandacht voor de volgende aspecten:
a. wat is de aard van het beveiligingsincident;
b. wat is de oorzaak dat dit beveiligingsincident heeft plaatsgevonden;
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.
2. De concernjurist maakt van het beveiligingsincident een verslag. Het verslag bevat in ieder geval de volgende informatie:
a. plaats in de organisatie 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.
3. De concernjurist beoordeelt 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);
4. Bestuur en management besluiten over het al dan niet doen van een melding;
5. De concernjurist doet namens de direct leidinggevende de melding aan de AP en aan de betrokkene(n);
6. De concernjurist is aanspreekpunt voor de AP en voorziet de AP voor zover noodzakelijk van nadere toelichting;
7. Eventuele aanwijzingen van de AP worden vastgelegd en opgevolgd;
8. De privacy en security officer legt een dossier aan van het beveiligingsincident en registreert dit in de beveiligingsincidentregistratie;

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

2.1.2 Meldingen verwerkers.
De gemeente laat bepaalde verwerkingen van persoonsgegevens geheel of gedeeltelijk uitvoeren door zogeheten verwerkers. Ondanks dat wij het “buitenshuis” plaatsen, zijn en blijven we verantwoordelijk voor deze verwerkingen. De AVG verplicht de gemeente 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 de gemeente aan deze meldplicht kan voldoen.
Met de verwerkers van onze gemeente wordt in verwerkersovereenkomsten afgesproken dat de verwerkers een incident/datalek direct na constatering melden bij de gemeente.
De melding bij de AP gebeurt door de concernjurist.

Bij een melding door een verwerker worden eveneens de stappen 1 tot en met 9 gevolgd vermeld onder 2.1.1.

2.1.3 Externe signalen / meldingen.
Een incident of datalek kan ook gesignaleerd/geconstateerd worden door een derde. Denk hier bijvoorbeeld aan een burger die een document met persoonsgegevens ontvangt die een andere persoon betreffen. Of een burger komt tot de ontdekking dat zij/hij via onze website toegang tot vertrouwelijke gegevens (persoonsgegevens) heeft die niet voor haar/hem bestemd zijn.
Burgers en ondernemers kunnen zich dan via de normale kanalen (brief, telefoon, loket, e-mail) wenden tot de gemeente.

Ook bij externe signalen/meldingen worden de stappen 1 tot en met 9 gevolgd vermeld onder 2.1.1.

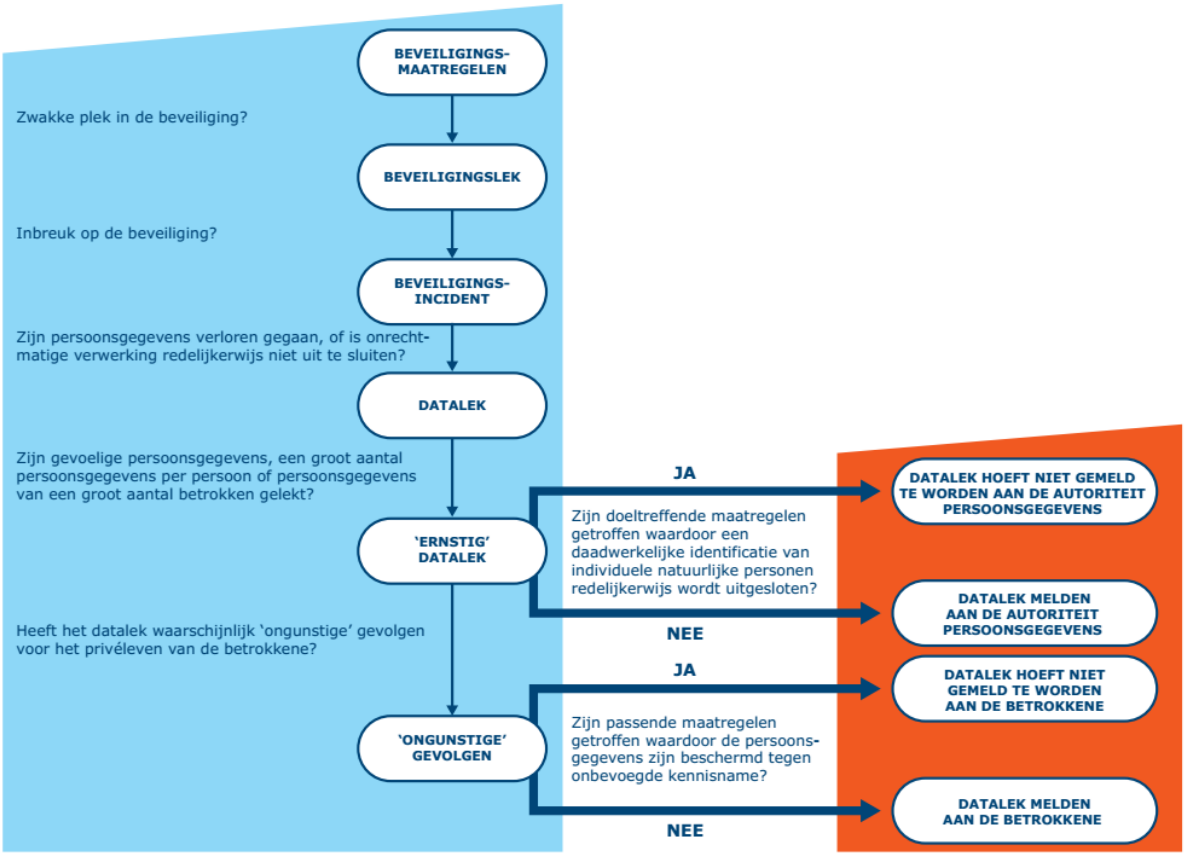
2.1.4 Het registreren van signalen / meldingen.
Zoals eerder aangegeven zullen alle gemelde incidenten geregistreerd worden. De security en privacy officer neemt deze registraties op in een register. In het register is onderscheidt gemaakt tussen ‘gemelde datalekken’, ‘niet gemelde datalekken’ en ‘registratie van beveiligingsincidenten’. De security en privacy officer draagt zorg voor het beheer van dit register en informeert het bestuur jaarlijks hierover.

2.2 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 privacy en security officer en de I&A-medewerkers van de Stafafdeling Middelen 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) 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.

2.3 Wanneer is er sprake van een datalek?
De Meldplicht datalekken staat opgenomen in de AVG. Alvorens te beoordelen of er sprake is van een datalek moet bekeken worden of de AVG van toepassing is en dus de meldplicht geldt.

Indien de meldplicht uit de AVG van toepassing is de tweede stap om na te gaan of in een bepaalde situatie sprake is van een datalek. Een datalek houdt een inbreuk op de beveiliging van persoonsgegevens in. Als verantwoordelijke ben je verplicht om passende technische en

organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.
Om vast te stellen of je een gebeurtenis moet beschouwen als een inbreuk op de beveiliging van persoonsgegevens (datalek) wordt hieronder afgebeelde stroomschema gebruikt.



2.4 Moet het datalek gemeld worden bij de AP en betrokkene(n)?
Bij de beslissing of een gebeurtenis die zich heeft voorgedaan gemeld moet worden aan de AP, en eventueel daarnaast ook aan de betrokkene(n), moet er een afweging plaatsvinden. Ook hierbij kan gebruik worden gemaakt van het hiervoor opgenomen stroomschema.

2.5 Het register datalekken en beveiligingsincidenten.
Alle meldingen van datalekken en incidenten worden geregistreerd. De privacy en security officer beheert het register. Zoals aangegeven onder paragraaf 2.1.4 worden ook niet gemelde datalekken geregistreerd.
De informatie uit meldingen wordt gebruik om het register te vullen. Verder worden in het register in ieder geval de volgende gegevens opgenomen:

- beschrijving van de inbreuk
- wie (melder)
- mogelijke gevolgen
- datum constatering
- meldingsdatum
- meldingsnummer AP
- reden niet melden bij AP
- opvolging/getroffen maatregelen/concrete maatregelen
- gemeld bij betrokkene(n)
- tekst kennisgeving aan betrokkene(n)

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

1. De leidinggevenden zorgen er voor dat het thema 'melding datalekken' voldoende aandacht krijgt, bijvoorbeeld in het werkoverleg of de terugkoppelingen van incidenten/datalekken.
2. De privacy en security officer 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 zijn/haar direct leidinggevende en de concernjurist;
4. De concernjurist is verantwoordelijk voor onderzoek en rapportage naar aanleiding van beveiligingsincident en betrekt hierbij de direct leidinggevende en de privacy en security officer;
5. De privacy en security officer is verantwoordelijk voor de advisering van de betrokken direct leidinggevende, eventueel het DT, MT, CMT en het bestuur over de mogelijke gevolgen van een beveiligingsincident voor de privacy van de betrokkene;
6. De direct leidinggevende verleent alle medewerking aan het onderzoek en is verantwoordelijk voor het ondernemen van preventieve en repressieve beveiligingsacties;
7. De concernjurist is de aangewezen contactpersoon met de AP en daarmee verantwoordelijk voor:

- de melding aan de AP en aan betrokkene;
- de communicatie met de AP en betrokkenen naar aanleiding van de meldingen.

2.7 Communicatie.

Bij datalekken of incidenten met een behoorlijke impact wordt de Adviseur Communicatie betrokken.

2.8 Het informeren van het bestuur.

Op het moment dat zich een datalek of beveiligingsincident voordoet beoordelen de concernjurist en de security en privacy officer of het noodzakelijk is de burgemeester en de gemeentesecretaris direct in te lichten.
Zodra een bepaald datalek of incident zodanig inbreuk maakt dat het aan een betrokkene moet worden gemeld, worden de burgemeester en de secretaris in ieder geval geïnformeerd door de concernjurist en de security en privacy officer.

Valkenburg, 7 mei 2019
Burgemeester en wethouders van Valkenburg aan de Geul,

L.T.J.M. Bongarts	dr. J.J. Schrijen
algemeen directeur / gemeentesecretaris,	burgemeester,