Gemeente Geertruidenberg

GEMEENTEBLAD

Officiële uitgave van de gemeente Geertruidenberg

Nr. 214002

10 oktober 2018

Procedure Meldplicht Datalekken & Veiligheidsincidenten gemeente Geertruidenberg

1. INLEIDING

1.1. Aanleiding

De meldplicht datalekken geldt in Nederland al sinds 2016. Onder de nieuwe Europese privacywet die sinds 25 mei 2018 geldt, de Algemene verordening gegevensbescherming (AVG), blijft de meldplicht datalekken bestaan. Deze meldplicht houdt in de gemeente 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 veiligheidsincidenten. Ingevolge de Baseline Informatiebeveiliging Gemeente (BIG) zijn wij verplicht om veiligheidsincidenten te registreren, zodat inzicht verkregen word en ervan geleerd wordt. Melding bij de AP van veiligheidsincidenten is niet verplicht.
Dit document voorziet in de procedure tot melding en registratie van datalekken en veiligheidsincidenten.

1.2 Wat is een datalek

Volgens de AVG is er sprake van een datalek als zich een inbreuk voordoet op de beveiligingsmaatregelen, wat leidt tot het per ongeluk, opzettelijk of onrechtmatig vernietigen, verliezen, aanpassen, ongeautoriseerde openbaring van, of toegang tot, persoonsgegevens die verwerkt zijn. Voorbeelden van datalekken zijn:

- het verlies van een mobiel apparaat (laptop, telefoon, Ipad 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 van het datalek 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 iedere datalek-incident 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 veiligheidsincident

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:

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

Hoofdstuk 2. PROCEDURE MELDPLICHT DATALEKKEN EN VEILIGHEIDSINCIDENTEN

Deze procedure beschrijft de wijze waarop binnen de gemeente Geertruidenberg wordt omgegaan met de meldplicht datalekken in de zin van de AVG en de registratie van veiligheidsincidenten ingevolge de BIG. Het bevat afwegingskaders bij een vermoeden van een datalek en specificeert de nodige acties.

In de procedure worden de volgende stappen in de procedure gehanteerd:
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 die 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 incidenten
2.1.1 Meldingen van medewerkers van de gemeente Geertruidenberg
Medewerkers van de gemeente kunnen incidenten/datalekken eenvoudig melden op VIA (intranet), bij de Functionaris Gegevensbescherming (FG) of de Chief Information Security Officer (CISO). Op VIA staat de volgende meldingsknop.

Figuur 1: meld een datalek
Zodra er op deze knop wordt geklikt verschijnt het formulier "Meld een datalek of incident", zie bijlage voor het formulier. Na het invullen van dit formulier kan het verzonden worden. De melding komt binnen op het e-mailadres: fg@geertruidenberg.nl. Deze mailbox wordt dagelijks uitgekeken door de FG, de Privacy officer (PO) en de CISO. Zij nemen de melding in behandeling.

Als er op een andere wijze gemeld wordt bij de FG of CISO, zal deze aan de medewerker vragen om te melden via VIA en het formulier "Meld een datalek of incident" in te vullen. Op deze wijze kunnen de meldingen beter geregistreerd worden.

Verder worden alle medewerkers op intranet en ook via andere communicatiekanalen regelmatig herinnerd aan de meldplicht datalekken en de registratie van veiligheidsincidenten en hierover geïnformeerd.

2.1.2 Meldingen verwerkers
Wij laten bepaalde verwerking 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 ons 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 wij aan deze meldplicht kunnen voldoen.
Met de verwerkers van de gemeente Geertruidenberg wordt in verwerkers overeenkomsten afgesproken dat de verwerkers een incident/datalek direct na constatering melden bij de FG via FG@geertruidenberg.nl.
De melding bij de AP gebeurd door de FG of CISO namens de burgemeester of het college van B&W.

2.1.3 Extern 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 be-

treffen. Of tot de ontdekking komt dat hij via onze website toegang tot vertrouwelijke gegevens (persoonsgegevens) heeft die niet voor hem bestemd zijn.
Bij dergelijke situaties is het belangrijk dat deze inwoners/ondernemers goed geïnformeerd worden over hoe ze moeten halen. Op de gemeentelijke website staat daarom informatie gepubliceerd hierover, zie bijlage 3. Ook wordt op de website aangegeven bij wie zij de constatering kunnen melden. Ook hier kan weer gemeld worden via fg@geertruidenberg.nl.

2.1.4 Het registreren van signalen / meldingen
Zoals eerder aangegeven zullen via intranet alle gemelde incidenten geregistreerd worden. De FG neemt deze registraties op in een register. In het register is onderscheidt gemaakt tussen 'gemelde datalekken', 'niet gemelde datalekken' en 'registratie van veiligheidsincidenten'. De FG draagt zorg voor het beheer van dit register en informeert het bestuur tweemaal per jaar hierover.

2.2 Het nemen van (beschermings)maatregelen
Na het signaleren/ontdekken van datalek/incident worden, indien mogelijk, direct passende technische en organisatorische beschermingsmaatregelen genomen. De FG en CISO analyseren de situatie en bekijken samen met het cluster Ondersteuning, team Automatisering welke beschermingsmaatregelen er genomen moeten worden om verdere inbreuk te voorkomen. In geval van veiligheidsincidenten kan hierover contact worden opgenomen met de Informatiebeveiligingsdienst (IBD) voor ondersteuning en advies.

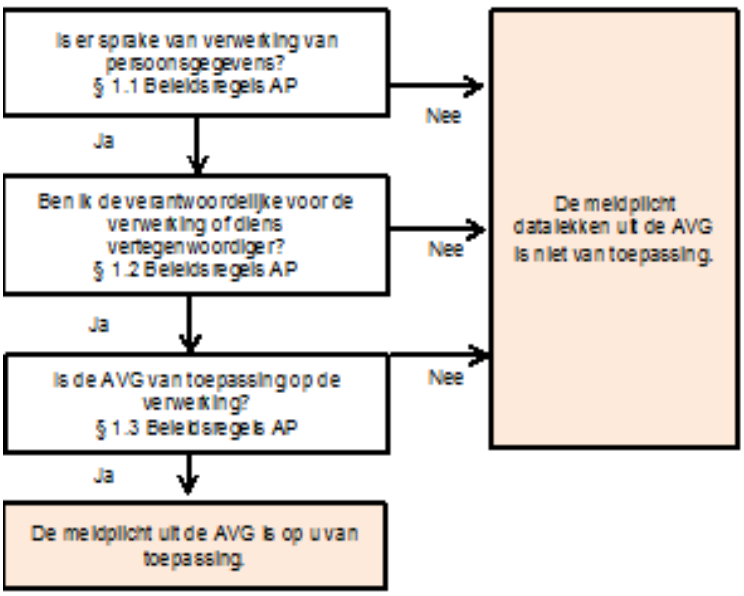
Hierbij kan gedacht worden aan bijvoorbeeld:
- het verwijderen van de persoonsgegevens (bijv. op afstand bij verloren mobiele apparaten);
- het aanpassen van de toegang tot de persoonsgegevens (autorisaties);
- het terugplaatsen van een back-up

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.

Daarvoor wordt het volgende stroomschema toegepast. Bij elke vraag wordt verwezen naar paragrafen uit Beleidsregels meldplicht datalekken van de AP. Bij onduidelijkheden kan dit dienen als naslagwerk/toelichting.

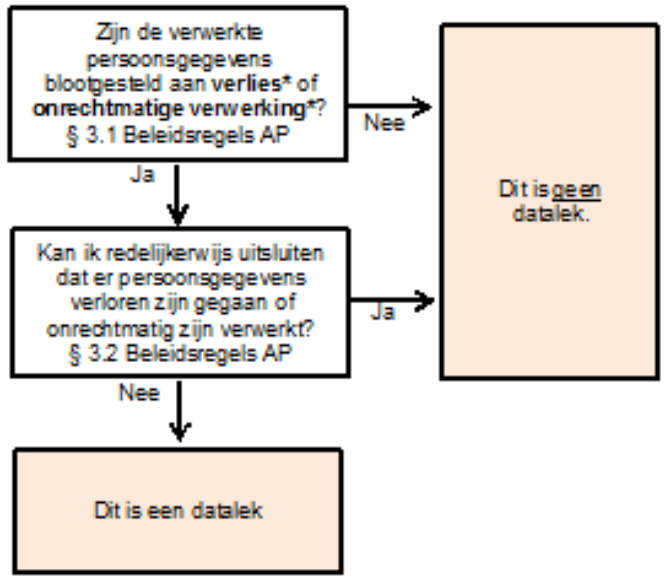
STAP 1: Is de AVG van toepassing op onderhavige constatering?



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) tref je hieronder een stroomschema.

STAP 2: Is er sprake van een datalek ingevolge de AVG?



*"Verlies houdt in dat je de gegevens niet meer hebt of tijdelijk niet over beschikt, omdat deze zijn vernietigd of op een andere manier verloren zijn gegaan.
*Onder onrechtmatige vormen van verwerking vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.

2.4 Moet de 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, moet er een aantal afwegingen gemaakt worden. Ook hierbij kan gebruik worden gemaakt van een stroomschema en de Richtsnoeren van de AP.

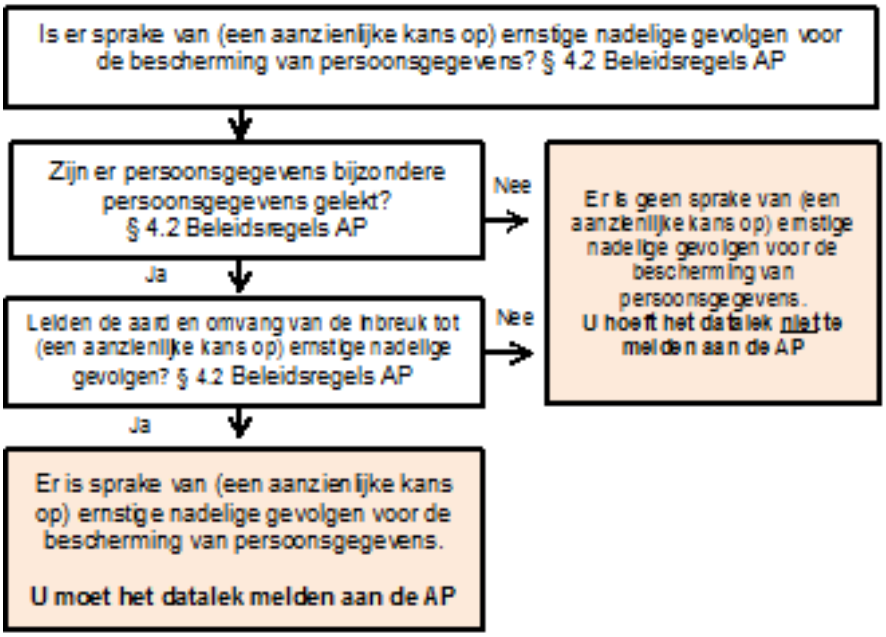
De FG, de CISO en de PO zullen aan de hand van de onderstaande vragen uit het stroomschema een beslissing nemen. Zij kunnen daarnaast gebruikmaken van de Beleidsregels meldplicht datalekken van de AP en de Guidelines Meldplicht datalekken. Beide documenten staat op de website van de AP gepubliceerd. De FG en de CISO zijn gemachtigd om namens het bestuur (college en burgemeester) een datalek bij de AP en de betrokkene te melden.

Deze functionarissen vormen samen met de PO het Team Datalekken.

Om deze afweging te maken kan het team input en/of advies vragen aan een beveiligingsbeheerder. In het informatiebeveiligingsbeleid zijn per onderwerp beveiligingsbeheerders aangewezen (Basisregistratie personen/Waardedocumenten, Basisregistratie Adressen en Gebouwen, Structuur uitvoeringsorgnisatie werk en inkomen (Suwinet), Digitale Identiteit (DigiD), Informatietechnologie (ICT) , Facilitaire Zaken (FZ) en Dienst Informatie Voorziening (DIV)).

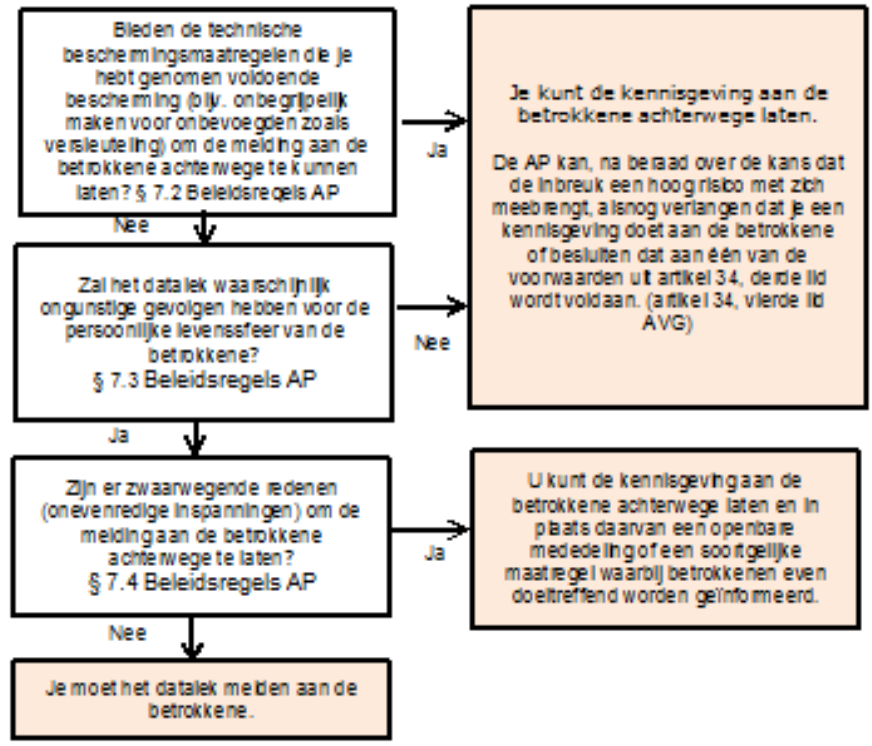
Nadat vastgesteld is dat het om een datalek gaat waar de AVG van toepassing op is, moeten worden nagegaan of het datalek gemeld moet worden bij de AP. Om vast te stellen of je een inbreuk moet melden tref je hieronder een stroomschema. Ook hier wordt weer verwezen naar de paragrafen uit de Beleidsregels meldplicht datalekken van de AP.

STAP 3: dient het datalek gemeld te worden bij de AP?



Nadat is vastgesteld dat een datalek gemeld moet worden bij de AP dient beoordeeld te worden of ook de betrokkene in kennisgeving gebracht moet worden. Artikel 34 van de AVG bepaald dat wanneer de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, de verantwoordelijke de betrokkene de inbreuk onverwijld moet melden.
Aan de hand van het onderstaande stroomschema kan je vaststellen of een specifiek datalek gemeld moet worden aan de betrokkene. In artikel 34, tweede lid en verder van de AVG, hoofdstuk 8 en 9 van de Beleidsregels meldplicht datalekken van de AP staat aangegeven wat, hoe en wanneer je dient te melden aan de betrokkene.

STAP 4: dient het datalek gemeld te worden bij de betrokkene(n)?



2.5 Het register datalekken en veiligheidsincidenten
Alle meldingen van datalekken en incidenten worden geregistreerd. De FG beheert het register. Zoals aangegeven onder paragraaf 2.1.4 worden ook niet gemelde datalekken geregistreerd.

De informatie uit meldingsformulieren wordt gebruik om het register te vullen. Verder bestaat het register in ieder geval uit de volgende kolommen:

- 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 Communicatie
Bij datalekken of incidenten met een behorlijke impact wordt cluster Advies, team Communicatie betrokken.

2.7 Het informeren van het bestuur
De burgemeester is de portefeuillehouder Privacy en Informatiebeveiliging. De FG en de CISO hebben structureel overleg met de burgemeester. Dan wordt de burgemeester bijgepraat over alle ontwikkelingen m.b.t. Privacy en Informatiebeveiliging. Ook op het gebied van datalekken en beveiligingsincidenten. Op het moment dat zich een lek of incident voordoet wordt beoordeeld of het noodzakelijk is om de burgemeester en de gemeentesecretaris direct in te lichten.

Zodra een bepaalde datalek of incident zodanig inbreuk maakt dat het aan een betrokkene moet worden gemeld, worden de burgemeester en de secretaris vooraf geïnformeerd door de FG of CISO.
Verder brengt de FG het register van Datalekken, zoals bedoelt onder paragraaf 2.5, tweemaal per jaar in het college.

Bijlage 1: Melding via Intanet voor medewerkers van de gemeente Geertruidenberg.
VIA-Juridisch
MELDEN DATALEK

Wat is een datalek?
We spreken van een datalek als persoonsgegevens in handen vallen van derden die hier geen toegang toe zouden mogen hebben. Ook is er sprake van een datalek als je niet kunt garanderen dat dit niet het geval is geweest. Het vernietigen of onbruikbaar maken van persoonsgegevens is eveneens een datalek. Een datalek is altijd het gevolg van een beveiligingsincident en kan per ongeluk of opzettelijk gebeuren. Een beveiligingsincident leidt tot een datalek als er persoonsgegevens bij betrokken zijn.

Voorbeelden van een datalek:
- een kwijtgeraakte USB-stick;
- een gestolen laptop, tablet of smartphone waarop persoonsgegevens staan.
- een inbraak door een hacker;
- verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden (bijv. bij email geen gebruik gemaakt van een BCC;
- een malware-besmetting of een phishing mail;
- een virus of ransomware aanval;
- het tijdelijk niet beschikbaar zijn van applicaties (m.u.v. vooraf gemelde updates);
- verdwenen dossiers of documenten waarop persoonsgegevens staan.

Meldplicht bij een datalek

Alle organisaties in Nederland – dus ook de gemeente Geertruidenberg – zijn verplicht om datalekken te melden bij de Autoriteit Persoonsgegevens (AP), als daaruit risico voortvloeit voor de betrokkenen. Ook moeten wij de benadeelde(n) van het datalek hierover informeren als er een kans bestaat op ernstig nadelige gevolgen voor hen. De AP is de toezichthouder op het gebied van privacy.
Bij een datalek is er sprake van overtreding van de AVG. Voor deze overtreding kan door de AP een hoge boete worden opgelegd. Omdat de wet strenge eisen stelt aan de termijn waarop wij doorgeven dat er een datalek is opgetreden (binnen 72 uur), is het belangrijk om een geconstateerd datalek direct, zonder uitstel, aan ons te melden via de rode knop “meld een datalek” op deze pagina. Ook als je twijfelt of er sprake is van een incident/datalek willen wij je vragen een melding te doen.

Je wordt na het drukken op de knop gevraagd om het meldingsformulier in te vullen en te verzenden. Het ingevuld formulier wordt dan automatisch verzonden naar de FG en de CISO. De manier waarop zij je melding afhandelen kun je vinden in de Procedure Meldplicht Datalekken en Veiligheidsincidenten Gemeente Geertruidenberg.

Bijlage 2: Interne meldingsformulier (intranet).
Melden van een datalek of een veiligheidsincidenten – Formulier melding
Gegevens van de melder

Naam:
Cluster:
Functie:
Email adres:

Omschrijving van het datalek of incident:

Om wat voor soort (persoons) gegevens / informatie gaat het?
Datum constatering datalek / incident:
Datum melding:

verzenden

Bijlage 3: privacymelding via internet voor de burgers en ondernemers.
Privacymelding

Dataveiligheid
De gemeente Geertruidenberg heeft een goede beveiliging van de persoonsgegevens die de gemeente gebruikt. Daarbij kijken wij steeds naar de huidige stand van de techniek en passen wij onze beveiliging daar op aan. Toch kan het gebeuren dat er inbreuk wordt gemaakt op onze beveiliging – bijvoorbeeld door een hack – waardoor persoonsgegevens in verkeerde handen komen. Dit heet een datalek. Op deze pagina vindt u meer informatie over datalekken, de meldplicht en wat u kunt doen als u denkt een datalek ontdekt te hebben binnen onze systemen.

Meldplicht datalekken
Alle organisaties in Nederland – dus ook de gemeente Geertruidenberg – zijn verplicht om datalekken te melden bij de Autoriteit Persoonsgegevens (AP), als daaruit risico voortvloeit voor de betrokkenen. Ook moeten wij de benadeelde(n) van het datalek hierover informeren als er een kans bestaat op ernstig nadelige gevolgen voor hen. De AP is de toezichthouder op het gebied van privacy.
Voor uitgebreide informatie over de meldplicht datalekken verwijzen wij u naar de website van de Autoriteit Persoonsgegevens.

Wat is een datalek?
Een datalek is een inbreuk op de beveiliging van persoonsgegevens, waardoor persoonsgegevens terechtkomen bij iemand die geen toegang tot die gegevens mag hebben of waardoor gegevens verloren gaan zonder dat er een back-up van de gegevens bestaat. Het kan bijvoorbeeld gaan om het hacken van digitale systemen van de gemeente waarbij persoonsgegevens worden gestolen, maar ook om een verloren USB-stick met adresbestanden of een gestolen laptop, tablet of smartphone waarop persoonsgegevens staan.

Hebt u een datalek ontdekt?
Hebt u via onze website toegang tot vertrouwelijke gegevens (zoals persoonsgegevens) die niet voor u bestemd zijn? Of zijn er bijvoorbeeld documenten met persoonsgegevens naar u verzonden die een andere persoon betreffen? Meld dit dan. Neem telefonisch contact op met de gemeente via telefoonnummer 14 0162 of mail naar FG@geertruidenberg.nl.
Let op: deel het datalek of zichtbare data niet met anderen.
Maakt u actief misbruik van een datalek of per abuis ontvangen persoonsgegevens? Dan doen wij aangifte bij de politie.

Wat doen wij als een datalek is ontdekt?
Dan is de eerste zorg het dichten van het lek. Tegelijkertijd gaan wij zorgvuldig na welke gegevens gelekt zijn en of de betreffende persoon mogelijk gedupeerd is door het lek. Als er een reëel risico is dat de privacy van de benadeelde geschonden is, melden wij het datalek bij de AP. Ook informeren wij in sommige gevallen de benadeelde(n) en helpen wij om het risico op schade uit het datalek te minimaliseren.