Datalekprotocol

Gemeente Gennep

gemeente
GENNEP

Inhoud

1. Afkortingen, Definities en omschrijvingen

AVG: Algemene Verordening Gegevensbescherming

UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming

Wpg: Wet politiegegevens

Inbreuk in verband met persoonsgegevens "datalek" (art. 4 sub 12 AVG): een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Melding: kennisgeving van een datalek aan de Autoriteit Persoonsgegevens (AP)

Autoriteit Persoonsgegevens (AP): De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. (zowel AVG als Wpg).

Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen

Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

Politiegegeven: persoonsgegevens die worden verwerkt voor de uitoefening van de politietaak.

De gemeente Gennep verwerkt in haar dienstverlenings- en bedrijfsvoeringsprocessen een omvangrijke hoeveelheid persoonsgegevens niet alleen van inwoners maar ook van medewerkers. Op de meeste verwerkingen van persoonsgegevens is de AVG van toepassing. Artikel 5 lid 1 sub f AVG, nader uitgewerkt in 32 van de AVG, bepaalt dat de verwerkingsverantwoordelijke beveiligingsmaatregelen treft die verlies of enige vorm van onrechtmatige verwerking moeten voorkomen.

Daarnaast verwerkt de gemeente Gennep politiegegevens. Dit zijn persoonsgegevens die verwerkt worden bij de uitvoering van politietaken. Ook de Wet politiegegevens (Wpg) (artikel 4a) bepaalt dat

de verwerkingsverantwoordelijke technische en organisatorische maatregelen dient te treffen om enige vorm van verlies of onrechtmatige verwerking te voorkomen.

Voor de gemeente Gennep is de BIO (Baseline Informatiebeveiliging Overheid) het uitgangspunt voor de te treffen maatregelen. De maatregelen bieden helaas geen garantie dat de beveiliging waterdicht is. Een doorbreking van de beveiliging is op zichzelf geen datalek. Er is pas sprake van een datalek als de doorbreking:

- óf leidt tot een aanzienlijke kans op nadelige gevolgen voor de privacy van de betrokkene
- óf dat er al nadelige gevolgen zijn voor de privacy van de betrokkene

Een inbreuk op de beveiliging van persoonsgegevens moet ruim worden genomen. Dit betreffen alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of de verwerkingsverantwoordelijke passende beveiligingsmaatregelen had getroffen of niet.

Voorbeelden van beveiligingsincidenten zijn:

- Een kwijtgeraakte of gestolen gegevenshouder zoals laptop of mobiel;
- Een inbraak door een hacker;
- Een verkeerde bijlage meegestuurd via een brief af als bijlage van een e-mail;
- Het delen van een document via Teams met iemand die geen toegang tot het document behoord te hebben;
- Het laten liggen van documenten met (gevoelige) persoonsgegevens bij de printer waardoor andere mensen het document zien;
- Een malware-besmetting;
- Een calamiteit zoals een brand, waardoor de gemeente geen toegang meer heeft tot bepaalde (persoons)gegevens.

Dit protocol geldt voor beveiligingsincidenten c.q. datalekken als bedoeld in de AVG en de Wpg.

2. Melding bij de Autoriteit Persoonsgegevens

In sommige gevallen moet een datalek worden gemeld bij de toezichthouder, de Autoriteit Persoonsgegevens (AP). Dit is het geval als uit het onderzoek naar een datalek blijkt dat het datalek een risico voor de rechten en vrijheden van natuurlijke personen inhoudt. Dit zal per geval moeten worden beoordeeld.

Bij twijfel kan een datalek beter wel worden gemeld.

Een datalek moet binnen 72 uur worden gemeld bij het digitale meldloket van de AP.

Uitzondering

De AP heeft een uitzondering geformuleerd waarbij geen melding hoeft te worden gedaan bij de AP, ondanks dat het datalek een risico voor de rechten en vrijheden van de betrokkene inhoudt. Dit is het geval als de persoonsgegevens aan een betrouwbare ontvanger zijn gelekt. Betrouwbaar houdt in dat je er redelijk zeker van kan zijn dat de onjuiste ontvanger geen kwaad in de zin heeft en dat hij zich houdt aan eventuele instructies om de persoonsgegevens terug te sturen of te verwijderen. Voorbeelden van betrouwbare ontvangers zijn partijen met een geheimhoudingsplicht of andere gemeenten. Dit moet per geval worden beoordeeld.

3. Melding aan de betrokkene

Volgens de AVG en Wpg stelt de verwerkingsverantwoordelijke de betrokkene onverwijld in kennis van de inbreuk op de beveiliging als die inbreuk waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van de betrokkene. Ook hierbij moet naar de feiten en omstandigheden van het geval worden gekeken en moet een afweging worden gemaakt hoe ernstig het datalek is. Daarbij spelen bijvoorbeeld de categorieën van persoonsgegevens die zijn gelekt een rol.

In dergelijke gevallen dient de verwerkingsverantwoordelijke de betrokkene in kennis te stellen van het datalek. Dit dient zo snel mogelijk te gebeuren om de mogelijkheid te hebben om zelf maatregelen te nemen of bekend te zijn met het risico.

Conform artikel 33a lid 6 en 7 Wpg zijn verschillende mogelijkheden om (tijdelijk) af te zien van het melden van het datalek aan de betrokkenen, bijvoorbeeld als de belangen op het gebied van opsporen en vervolgen zwaarder wegen.

4. Taken, verantwoordelijkheden en bevoegdheden

Taken, verantwoordelijkheden en bevoegdheden zijn binnen deze procedure als volgt georganiseerd:

Iedere **medewerker** die direct of indirect kennis draagt of krijgt van een mogelijk beveiligingsincident, is verplicht dit direct te melden via de servicedesk of bij de servicedeskmedewerker als het gaat om een ICT gerelateerde melding of anders bij de verantwoordelijk manager én Privacy Officer (PO) of Chief Information Security Officer (CISO). De medewerkers vult direct het Meldingsformulier datalekken in en levert dit aan bij de PO of CISO én verantwoordelijke manager.

De **verantwoordelijk manager** verleent alle medewerking aan het onderzoek en is verantwoordelijk voor:

- het tijdig (laten) invullen van het meldingsformulier en de aanlevering daarvan bij de PO en/of CISO;
- het ondernemen van preventieve en repressieve beveiligingsacties;
- de melding aan- en communicatie met betrokkene.

De **Privacy Officer (PO)** is verantwoordelijk voor:

- de actualiteit van deze procedure, de bekendmaking en het in kennis stellen c.q. instrueren van de medewerkers.
- onderzoek en rapportage maar aanleiding van beveiligingsincident;
- consultatie van de Functionaris Gegevensbescherming (FG);
- voor de advisering van het betrokken management en het bestuur over de mogelijke gevolgen van een beveiligingsincident voor de privacy van de betrokkene.
- De interne registratie van het incident;
- het bewaken van termijnen, waaronder de (eerste) melding binnen 72 uur na ontdekken.
- de melding aan de AP;

De **Chief Information Security Officer (CISO)** is verantwoordelijk voor:

- onderzoek en rapportage naar aanleiding van beveiligingsincident;

De **Functionaris Gegevensbescherming (FG)** is verantwoordelijk voor:

- advisering bij het datalek/beveiligingsincident.
- toezicht op de procedure.
- contactpersoon voor de AP.

De gemeente Gennep beschikt over een structuur voor incident- of crisisbeheer. Dit is vastgelegd in het Incidentmanagement. De crisisorganisatie opereert onder de directe verantwoordelijkheid van het College van Burgemeester en Wethouders. Op ambtelijk niveau is er een Crisisbeheerteam (CBT) bestaande uit de gemeentesecretaris als crisiscoördinator, de afdelingsmanagers, afgevaardigde OOV, communicatie en ICT. Het CBT fungeert als het **Datalek respons team**: Dit CBT komt uitsluitend bij elkaar in geval van grote beveiligingsincidenten, datalekken of calamiteiten. Afhankelijk van het type crisis zal het CBT een beroep doen op medewerkers of andere benodigde expertise of deskundigheid zoals de CISO, PO, FG en zo nodig andere experts.

5. Uitvoering

De uitvoeringsfase kent de volgende onderdelen:

1. De medewerker die direct of indirect kennis draagt of krijgt van een beveiligingsincident meldt dit direct aan de PO of CISO én de verantwoordelijk manager. Dit kan via een melding servicedesk of rechtstreeks. Een ICT-gerelateerd incident wordt direct (mondeling) gemeld via de service-desk.

2. De medewerker vult het meldingsformulier datalekken in en verstrekt dit aan de PO of CISO en de verantwoordelijk manager. Zie hiervoor bijlage 4.

3. De CISO, PO en de beveiligingsbeheerder van het specifieke vakgebied, onderzoeken het beveiligingsincident. Hierbij is aandacht voor de volgende aspecten:

- Wat is de aard van het beveiligingsincident?

- Wat is de oorzaak dat dit beveiligingsincident heeft plaatsgevonden?
- Is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures?
- Is er sprake van verwijtbaar handelen en door wie?
- Zie ook de vragen in bijlage 3, die bijdragen aan het verschaffen van overzicht in de situatie.

4. De CISO of PO maakt van het beveiligingsincident een verslag. Het verslag bevat in ieder geval de volgende informatie:
- De plaats in de organisatie waar het beveiligingsincident zich heeft voorgedaan, op welk informatiesysteem en of er persoonsgegevens zijn betrokken bij het beveiligingsincident.
- Een beschrijving van het beveiligingsincident.
- Opgave van de categorieën van personen waarvan de (bijzondere) persoonsgegevens betrokken zijn in het beveiligingsincident.
- Inzicht in de getroffen maatregelen die genomen zijn om eventuele gevolgen te beperken.
- Inzicht in de getroffen maatregelen om dergelijke beveiligingsincidenten in de toekomst te voorkomen.

5. De PO beoordeelt (eventueel ondersteund door de FG en CISO) 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 betrokkenen.

6. Indien er sprake is van een groot incident of calamiteit komt het Crisisbeheerteam (CBT) bij elkaar. Dit team doet onderzoek naar het datalek en treft de noodzakelijke maatregelen in het kader van risicobeheersing. Het team coördineert de te treffen maatregelen en draagt zorg voor de communicatie, intern en extern.

7. De burgemeester (als portefeuillehouder privacy en beveiliging persoonsgegevens) besluit over het al dan niet doen van een melding. De FG en/of CISO kan een zwaarwegend advies geven.

8. De PO doet de melding aan de AP en de verantwoordelijk manager doet melding aan de betrokkenen, zo spoedig mogelijk maar uiterlijk binnen 72 uur na ontdekken.

9. De FG is aanspreekpunt voor de AP en voorziet de AP voor zover noodzakelijk van nadere toelichting.

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

11. De PO legt een dossier aan van het beveiligingsincident, registreert dit in de beveiligingsincidentregistratie en archiveert dit in het zaaksysteem. De bewaartermijn is 5 jaar na afhandeling.

Let op: onder de AVG en Wpg moeten alle datalekken gedocumenteerd worden, ook datalekken die niet gemeld hoeven te worden bij de AP of de betrokkene.

6. Interne controle

De interne controle geschiedt als volgt:

Op basis van de binnen een jaar tijd ontvangen meldingen, analyseren de CISO, de PO en de FG deze en stellen samen een verbeter- of adviesplan op. Dit plan of advies wordt opgenomen in de jaarlijks uit te brengen managementrapportage.

Minimaal jaarlijks beoordeelt de FG of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de procedure.

7. Toelichting op de term "verwerker"

Een verwerker is een natuurlijke persoon of rechtspersoon die ten behoeve van verwerkingsverantwoordelijke persoonsgegevens verwerkt. Voorbeelden van dat soort werkzaamheden zijn de uitbesteding van invorderingstaken of parkeerbeheer.

Verwerkingsverantwoordelijke en de verwerker leggen in een (verwerkers)overeenkomst vast aan welke eisen van beveiliging de verwerker moet voldoen. De verwerker dient verwerkingsverantwoordelijke in staat te stellen om te kunnen voldoen aan diens verplichtingen, in het kader van het melden van datalekken. Verwerkingsverantwoordelijke en verwerker kunnen overeenkomen dat de verwerker namens verwerkingsverantwoordelijke op een vergelijkbare wijze als beschreven in deze procedure, invulling geeft aan de meldplicht. Verwerkingsverantwoordelijke is verplicht de nakoming van de afspraken te controleren.

Procedure datalek bij verwerker

In de meeste gevallen is in de verwerkersovereenkomst afgesproken dat de verwerker een mogelijk datalek binnen 24 uur bij de gemeente Gennep als verwerkingsverantwoordelijke meldt. Als de verwerker een dergelijke melding doet worden dezelfde stappen genomen als beschreven in hoofdstuk 5. Alleen komt de melding dan niet binnen via het meldingsformulier of een collega, maar via de verwerker. Op het moment dat de gemeente Gennep vaststelt dat sprake is van een datalek, begint de termijn van 72 uur om het datalek te melden aan de toezichthouder te lopen.

8. Aanvullende informatie

- De bewaartermijn van 5 jaar is afkomstig uit Selectielijst gemeenten en intergemeentelijke organen 2020, 26 februari 2020: categorie 29.1, 5 jaar na afhandeling
- De bewaartermijn van maximaal 5 jaar voor politiegegevens is afkomstig uit artikel 14 van de Wet politiegegevens.

BIJLAGE 1:STAPPENPLAN

AUTORITEIT
PERSOONSGEGEVENS

Stappenplan: kom in actie bij een datalek

Heeft uw organisatie te maken met een datalek? Dan is het belangrijk dat u als privacycontactpersoon snel in actie komt. Met dit stappenplan helpen we u op weg.

Stap 1: zorg voor overzicht

Analyseer onmiddellijk de situatie. Zorg dat u weet wat er is gebeurd en wat de omvang van het lek is. Gaat het om een inbreuk door gelekte, vernietigde of gewijzigde gegevens? Indien gegevens zijn gelekt, onderzoek dan wie er (mogelijk) toegang hebben (gehad) tot welke persoonsgegevens. Deze informatie heeft u nodig voor de vervolgstappen.

Stap 2: Beperk de schade!

Bepaal op basis van stap 1 of er maatregelen zijn die u meteen kunt nemen om het datalek te beëindigen en de schade te beperken. En zo ja, neem deze maatregelen onmiddellijk. Bijvoorbeeld door een gestolen laptop op afstand te wissen. Maak tegelijkertijd een inschatting van het (mogelijke) risico dat het datalek oplevert (stap 3).

Stap 3: Wel/niet melden bij de AP

Bepaal of u het datalek verplicht moet melden bij de Autoriteit Persoonsgegevens (AP). Zo ja, zorg dat u dit ***binnen 72 uur*** nadat u het lek heeft ontdekt doet. U moet een datalek melden bij de AP tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen.

Heeft u bij de eerste melding nog niet alle informatie over het datalek?
Doe dan een eerste melding binnen 72 uur en doe later een vervolgmelding.

Naar het meldloket datalekken
Zie ook: voorbeeldlijst 'datalek wel/niet melden bij AP en betrokkenen'

Stap 4: Wel/niet melden aan de betrokken personen

Bepaal of u het datalek verplicht moet melden aan de betrokken personen. Zo ja, zorg dat u dit zo snel mogelijk doet. U moet een datalek melden aan de betrokken personen wanneer er sprake is van een *hoog* risico voor de rechten en vrijheden van de betrokken personen.

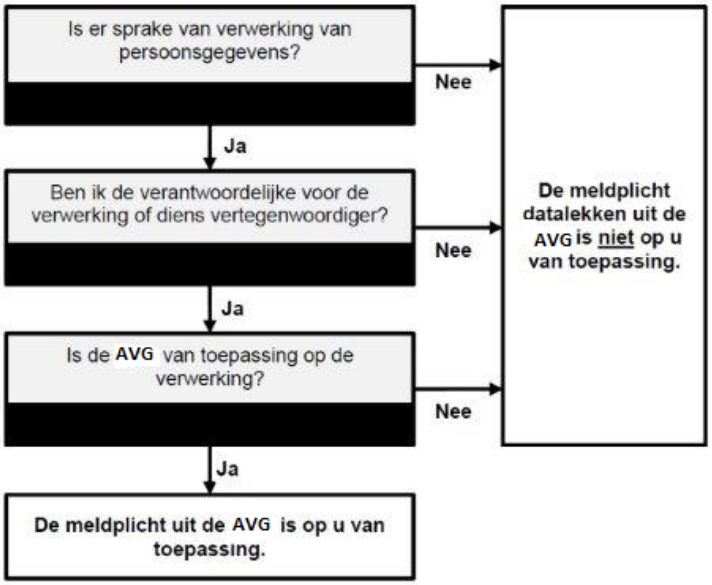
Stap 5: Registreer het datalek

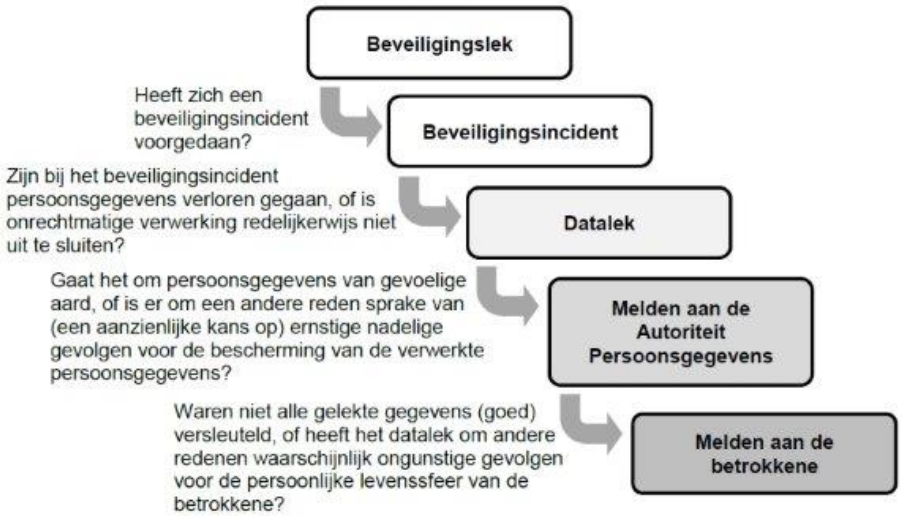
Registreer het datalek in uw verplichte datalekregister. Ook wanneer u het datalek niet meldt aan de AP.

Zie ook: 10 praktische tips voor betere datalekregistratie

Heeft u bovenstaande stappen doorlopen? En alles gedaan om de schade te beperken?
Start dan een evaluatie om een herhaling van het datalek te voorkomen.

BIJLAGE 2: BESLISBOOM





BIJLAGE 3 EEN DATALEK, WAT TE DOEN?

Is er sprake van een datalek, dan moeten de eerste acties erop gericht zijn om het datalek te beëindigen en de eventuele negatieve gevolgen voor de betrokken personen te beperken.

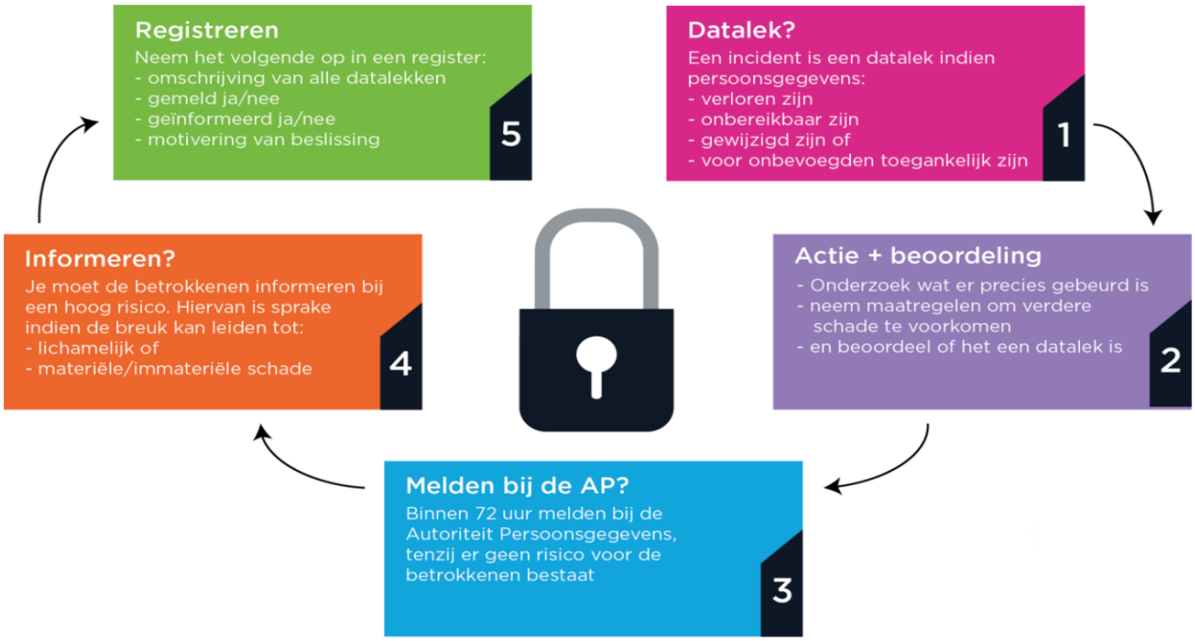
Door beantwoording van de volgende vragen kan overzicht worden verkregen van de situatie

1. Om wat voor soort datalek gaat het?
2. Wat is de oorzaak van het datalek?
3. Wanneer is het datalek ontstaan? En bestaat het lek nog steeds?
4. Hoe lang na het ontstaan van het datalek is het ontdekt? En hoe is het ontdekt?
5. Wat voor soort persoonsgegevens zijn er gelekt? Bijvoorbeeld naam, adres, e-mailadressen, politiegegevens, creditcardgegevens en/of bijzondere persoonsgegevens.
6. Hoeveel persoonsgegevens zijn er (bij benadering) gelekt? Om hoeveel personen gaat het?
7. Om wat voor groepen mensen gaat het? Bijvoorbeeld klanten, werknemers, scholieren, patiënten, inwoners etc. Gaat het om kwetsbare groepen? Bijvoorbeeld kinderen, gehandicapten of bejaarden.
8. Hoeveel onbevoegden hadden of hebben bij benadering (mogelijk) toegang tot de gelekte persoonsgegevens?
9. Heeft u zicht op wie de onbevoegden zijn? En is het waarschijnlijk dat de onbevoegden kwade bedoelingen hebben met de gegevens? Of gaat het om een bekende, betrouwbare ontvanger?
10. Heeft uw organisatie vooraf maatregelen getroffen waardoor de gelekte persoonsgegevens (deels) ontoegankelijk zijn voor onbevoegden? Bijvoorbeeld omdat de gegevens versleuteld zijn?

In de Algemene verordening Gegevensbescherming (AVG) wordt een datalek een inbreuk in verband met persoonsgegevens genoemd.

Er komt een melding binnen van datalek. Hoe weten we of we dit moet melden bij de Autoriteit Persoonsgegevens (AP) en of we de betrokkenen moet informeren? Want niet ieder datalek hoeft gemeld te worden, maar hoe zit dat nou precies?

Dit schema en de checklist helpt ons bij de beoordeling.



Belangrijk:

- Mocht er sprake zijn van een (mogelijke) crisis of calamiteit wordt door de CISO opgeschaald naar de crisisorganisatie en wordt het Crisis Beheer Team (CBT) ingesteld.
- Communiceer met elkaar over wie wat wanneer communiceert. We willen dat de gevolgen van melding en het eventuele datalek beheersbaar blijven.

Tref maatregelen om het lek te dichten en de gevolgen te beperken

- Stel vast welke maatregelen getroffen moeten worden om het lek te dichten (corrigerende maatregelen) en zorg dat het lek zo spoedig mogelijk wordt gedicht
- Stel vast welke maatregelen noodzakelijk of wenselijk zijn ter beperking van eventuele nadelige gevolgen voor betrokkenen (preventieve maatregelen)
- Benoem de technische en organisatorische maatregelen die zijn of worden getroffen om (dezelfde soort) datalekken in de toekomst te voorkomen en laat deze vaststellen door de afdelingsmanager.

De afdelingsmanager wordt geadviseerd de maatregelen te implementeren en blijvend te monitoren en te evalueren op effectiviteit, in relatie tot de bescherming persoonsgegevens.

Verzamel alle relevante informatie

Het is belangrijk om alle relevante informatie over het (vermeende) datalek te verzamelen. Wat is er gebeurd en wanneer, de aard van de inbreuk, de categorieën van persoonsgegevens en de categorieën van betrokkenen.

Beoordeel het risico aan de hand van de volgende relevante factoren:

- De aard van de inbreuk (wat is er precies gebeurd?)
- Aard, gevoeligheid en het aantal persoonsgegevens of bijzondere persoonsgegevens of gegevens van vertrouwelijke aard[1]
- Gemak waarmee personen kunnen worden geïdentificeerd
- Ernst van de gevolgen voor personen
- Kwetsbaarheid van getroffen personen (zoals kinderen of zieken)
- Het aantal getroffen personen (is er een risico te verwachten, dan dien je dit te melden via het formulier op de website van de AP).
- Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie

Beoordeel of het datalek gemeld moet worden bij de AP

Een datalek moet binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens (AP), als het datalek een risico inhoudt voor de rechten en vrijheden van de getroffenen.

Beoordeel of de betrokkenen moeten worden geïnformeerd

Wanneer uit de beoordeling blijkt dat het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokken personen moeten betrokkenen worden geïnformeerd.

- Er is sprake van een hoog risico als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen. (bijv. discriminatie, identiteitsdiefstal of –fraude, financieel verlies en reputatieschade)
- Ga na of de betrokkene zichzelf beter kan beschermen indien hij de inbreuk kent (denk aan inloggegevens die op straat zijn beland)

Informeren van betrokkenen is niet vereist indien is voldaan bij één van deze omstandigheden:

- de getroffen persoonsgegevens zijn adequaat onbegrijpelijk of ontoegankelijk gemaakt door verwerkingsverantwoordelijke (bijv. door versleuteling met de nieuwste technieken)
- er zijn achteraf maatregelen genomen waardoor het onwaarschijnlijk is geworden dat het hoge risico zal intreden (bijv. gegevens worden op afstand gewist en het is zeker dan de gegevens niet zijn gebruikt)

1

1 Godsdienst of levensovertuiging, ras of etnische afkomst, politieke opvattingen, gezondheid, seksuele leven, lidmaatschap vakbond, strafrechtelijk verleden en genetische of biometrische gegevens met oog op unieke identificatie.

2 Financieel of economisch, stigmatiserend, specifieke problemen, school of werkprestaties, inloggegevens, gegevens die bruikbaar zijn voor identiteitsfraude, gegevens die vallen onder beroepsgeheim.

- betrokkenen informeren zou een onevenredige inspanning vergen (bijvoorbeeld als het een groot aantal betrokkenen betreft); in dat geval volstaat een openbare mededeling

Let op! Als je niet informeert, leg dit dan vast met een onderbouwing.

NB: de AP kan na ontvangst van een melding de verwerkingsverantwoordelijke verplichten om betrokkenen (alsnog) te informeren, als dat nog niet is gebeurd.

gemeente GENNEP

Meldingsformulier datalekken gemeente Gennep

GEGEVENS MELDER

Naam	
Functie	
Afdeling	
Contactgegevens	

GEGEVENS INCIDENT

Op welke datum heeft het incident plaatsgevonden?	
Op welke datum heb je het incident ontdekt?	
Op welke datum heb je het incident gemeld bij de CISO, PO of FG?	
Welke persoonsgegevens zijn er bij het incident betrokken? (Algemene-, bijzondere en/of strafrechtelijke persoonsgegevens)	
Op welk bestand of applicatie heeft het incident betrekking?	
Van wie zijn de persoonsgegevens gelekt?	
Wat is de omvang van het datalek?	
Beschrijf het incident. (Doe dit zo precies mogelijk. Geef daarbij aan of het om gelekte, vernietigde of gewijzigde gegevens gaat)	
Wie hebben er mogelijk toegang tot welke gegevens gehad?	

Wat heb je gedaan om het datalek te beëindigen of schade te beperken? (Welke maatregelen zijn genomen?)	
Welk(e) (mogelijke) risico(s) levert het datalek op?	

GEGEVENS BETROKKENE(N)

Wie zijn door de melder geïnformeerd en wanneer?	
Welke acties of toezeggingen zijn gedaan?	

EVALUATIEFORMULIER DATALEKKEN

BEHORENDE BIJ:	
Onderwerp:	
Datum:	
Zaaknummer:	

BEWUSTWORDING

Wanneer is het incident besproken binnen het betreffende team/afdeling?	
Hoe had het incident voorkomen kunnen worden?	
Welke leerpunten zijn hieruit gekomen?	
Welke maatregelen zijn genomen?	

Handtekening melder: .....

BIJLAGE 5 CONTROLE FG _PROCEDURE VS UITVOERING

datum	**Akkoord/opmerkingen**	**paraaf**
1-11-2021	vastgesteld	FC
1-10-2022	akkoord	FC
1-10-2023	Niet akkoord, zie opmerkingen. Advies: Update procedure	FC
1-10-2024