Protocol melding datalekken en beveiligingsincidenten

1 Inleiding

Om een zorgvuldige omgang met gegevens binnen de gemeenten Alphen-Chaam, Baarle-Nassau, Gilze en Rijen en de ABG-organisatie (tezamen hierna te noemen: 'Organisatie') te waarborgen is het navolgende protocol "Melding datalekken en beveiligingsincidenten" vastgesteld. Het beschrijft eerst in de werkinstructies ten aanzien van het hoe te handelen als er zich een beveiligingsincident en/of datalek heeft voorgedaan onder de kop "3. Procedure melden van beveiligingsincidenten". Vervolgens legt het instructies neer over hoe datalekken dienen te worden afgehandeld waar persoonsgegevens mee zijn gemoeid en wanneer de Autoriteit Persoonsgegevens en eventueel de betrokkene dienen te worden geïnformeerd onder "4. Procedure melden van datalekken".

2 Algemene bepalingen

2.1 Doelstelling

Informatiebeveiliging: Conform de BIG (Baseline Informatiebeveiliging Gemeenten) hanteert de Organisatie de volgende doelstellingen:

- Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
- De procedure voorziet in de gestructureerde en vastgelegde werkwijze voor het melden en registreren van (bijna) incidenten.
- Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

2.2 Bekendmaking

De inhoud van deze procedure moet bekend zijn bij alle medewerkers van de Organisatie. Dit geldt dus ook voor de extern ingehuurde medewerkers.

2.3 Definities

Wet bescherming persoonsgegevens (hierna te noemen 'Wbp')

De Wbp is de Nederlandse uitwerking van de 'Europese richtlijn bescherming persoonsgegevens' (richtlijn 95/46/EG) en reguleert de omgang met persoonsgegevens in Nederland. De wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om in een bestand te worden opgenomen. Op 25 mei 2018 komt de Wbp te vervallen door de komst van de AVG.

Algemene Verordening Gegevensbescherming (hierna te noemen 'AVG')
De AVG of GDPR in de Engelse Terminologie, is een Europese Verordening die vanaf 25 mei 2018 rechtstreeks gaat gelden in alle lidstaten van de Europese Unie. Vanaf deze datum komt de voornoemde Wbp als zodanig te vervallen. Voor Nederland verandert de komst van de AVG niet veel ten opzichte van de Wbp. Wat wel veranderd, is een uitbreiding van de bevoegdheden van de Autoriteit Persoonsgegevens als het gaat om het uitdelen van boetes en de verplichting aan organisaties om de door hen getroffen maatregelen ten aanzien van de bescherming van persoonsgegevens (beter) te documenteren. Door het laatste moeten organisaties kunnen aantonen dat ze voldoen aan de vereisten van de wetgeving.

Autoriteit Persoonsgegevens (hierna te noemen 'AP')
De AP is een nationale, onafhankelijke autoriteit, die toezicht houdt op het verwerken van persoonsgegevens, zoals bepaald in de AVG en diens voorganger (de Europese privacyrichtlijn waarop de Wbp is gebaseerd). De AP heeft de bevoegdheid om boetes op te leggen als organisaties de AVG of (tot 25 mei 2018) de Wet bescherming persoonsgegevens overtreden.

Persoonsgegeven
Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dit houdt in dat het gaat om ieder gegeven waarmee een individu van anderen kan worden onderscheiden. Het kan gaan om een naam, adres, BSN-nummer of een (of een combinatie van) element(en) die kenmerkend zijn voor een specifiek persoon. (artikel 4 lid 1 AVG)

Verwerking van persoonsgegevens
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals 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. (artikel 4 lid 2 AVG)

Datalek
De term datalek is in de AVG opgenomen als een "inbreuk in verband met persoonsgegevens". Dit wordt omschreven als "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" (artikel 4 lid 12 AVG). Hoewel een datalek geen betrekking hoeft te hebben op persoonsgegevens, kan het vaak niet worden uitgesloten dat er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. Om deze reden wordt een datalek hier in verband gebracht met (de beveiliging van) persoonsgegevens.

Beveiligingsincident
Iedere gebeurtenis die schade toebrengt of kan toebrengen aan de beveiliging van informatie. Hiermee wordt bedoeld iedere inbreuk op het gebied van beschikbaarheid, betrouwbaarheid,

vertrouwelijkheid en/of controleerbaarheid van gegevens. Niet ieder beveiligingsincident is een datalek. Een (mislukte) aanval op een geautomatiseerd systeem, waarbij geen toegang is verkregen tot gegevens dient bijvoorbeeld wel geregistreerd te worden als een beveiligingsincident, maar is geen datalek. Andersom kan een onbewuste en onbedoelde operationele fout leiden tot een datalek, maar kan voorkomen zonder dat er sprake is van een beveiligingsincident.

Melding
De kennisgeving van een datalek of beveiligingsincident aan een betreffende autoriteit. Dit kan gaan om de IBD (Informatie Beveiligingsdienst), de RVIG (Rijksdienst voor Identiteitsgegevens), en/of de Autoriteit Persoonsgegevens (AP). Ook de betrokkene, degene waar de persoonsgegevens betrekking op hebben, dient in bepaalde gevallen geïnformeerd te worden d.m.v. een melding. Dient de AP te worden geïnformeerd, dan dient deze melding onverwijld en uiterlijk binnen 72 uur te gebeuren aan het AP, de betrokkene zo spoedig mogelijk.

Chief Information Security Officer (hierna te noemen 'CISO')
Het is de taak van de CISO om op basis van de algemeen aanvaarde standaard de Baseline Informatiebeveiliging Gemeenten (BIG), zorg te dragen voor een samenhangend pakket van technische en organisatorische maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente. Risicoanalyse, oog voor de bedrijfsvoering en in achtneming van de wettelijke voorschriften zijn daarbij sleutelbegrippen.

3 Procedure melden van beveiligingsincidenten

3.1 Implementatie
Conform de BIG:

- Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.
- Er is een procedure voor communicatie met de Informatiebeveiligingsdienst (IBD).
- Er is een contactpersoon aangewezen voor het rapporteren van beveiligingsincidenten.
- Alle beveiligingsincidenten worden vastgelegd in een systeem.
- Alle relevante beveiligingsincidenten worden geëscaleerd aan de Informatiebeveiligingsdienst van KING.
- Vermissing of diefstal van apparatuur of media die gegevens van de gemeente kunnen bevatten, wordt altijd aangemerkt als informatiebeveiligingsincident.
- Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De CISO bekijkt periodiek – bij voorkeur maandelijks - een samenvatting van de informatie.
- Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.

- Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

3.2 Over beveiligingsincidenten

Met betrekking tot het rapporteren van beveiligingsincidenten behoort rekening te worden gehouden met de volgende situaties:

- niet-doeltreffende beveiligingsbeheersmaatregelen;
- schending van informatie-integriteit, vertrouwelijkheid of aanwezige verwachtingen;
- menselijke fouten;
- niet-naleving van beleidsregels of richtlijnen;
- schending van fysieke beveiligingsregelingen;
- onbeheerste systeemveranderingen;
- storingen in soft- of hardware, berichtenverkeer, netwerk;
- overtredingen van de logische of fysieke toegangsbeveiliging.

Mogelijke beveiligingsincidenten zijn o.a.:

- Uitlekken van gevoelige informatie zoals een kwijtgeraakte USB stick per persoonsgegevens;
- bedreiging of intimidatie (extern of intern);
- onbevoegde aanwezigheid;
- diefstal met of zonder geweld;
- interne fraude;
- diefstal met of zonder braak;
- meervoudige vermissing van reisdocumenten/rijbewijzen;
- verdacht postpakket;
- fraude door de klant (bv. look alike / vingerafdrukken / valse brondocumenten;
- (hack) exploit;
- verstoring van de beschikbaarheid van IT systemen door bijvoorbeeld een DDOS aanval;
- calamiteiten zoals brand in de serverruimte of brandstichting in de publieksruimte.

3.3 Beheersmaatregel

Verantwoordelijkheden en procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen. Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de voorliggende gedocumenteerde procedure.

3.4 Prioritering van beveiligingsincidenten

De prioriteit van een incident wordt meestal bepaald door de beoordeling van de impact en urgentie, waarbij:

- urgentie de maat is voor hoe snel de oplossing van het incident vereist is.

- impact de maat is voor de omvang van het incident en van de mogelijke schade als gevolg van het incident voordat het kan worden opgelost.

Urgentie van incidenten

In de linker kolom van onderstaande tabel worden urgentiecategorieën beschreven. Om de urgentie van een incident vast te stellen, kiest u de van toepassing zijnde waarde van de desbetreffende categorie:

Categorie	Omschrijving van de urgentie
Hoog (H)	De schade veroorzaakt door het incident neemt snel toe. Werk dat moet worden hersteld door personeel is zeer arbeidsintensief. Een groot incident kan worden voorkomen door bij een klein incident onmiddellijk te handelen.
Medium (M)	De schade veroorzaakt door het incident neemt in de tijd aanzienlijk toe. Er gaat werk verloren, maar dit is relatief snel te herstellen.
Laag (L)	De schade veroorzaakt door het incident neemt in de tijd maar weinig toe. Het werk dat blijft liggen is niet tijdsintensief.

Impact van het incident

Om de impact van het incident vast te stellen, kiest u de van toepassing zijnde incident impact categorie.

Categorie	Omschrijving
Hoog (H)	Relatief veel personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen. Meerdere organisatieonderdelen zijn geraakt, de publieksbalie moet gesloten worden. Burgers of bedrijven zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn in het geding (datalek melden). De financiële impact van het incident is hoger dan €10.000,-. Er is reputatieschade, de krant wordt gehaald. Er zijn lichamelijk gewonden.
Medium (M)	Enig personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen, bijvoorbeeld een afdeling.

Categorie	Omschrijving
	Enkele inwoners zijn geraakt en/of lijden schade op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn in het geding, maar de schade kan snel worden gerepareerd. De financiële impact van het incident is hoger dan €1.000,- en lager dan €10.000,-. Er is kans op reputatie schade.
Laag (L)	Enkele personeelsleden zijn geraakt door het incident en/of kunnen hun werk niet meer doen. Enkele burgers zijn minimaal geraakt en/of lijden minimale schade. De financiële impact van het incident is lager dan €1.000,- Er is geen kans op reputatie schade.

Incident Prioriteiten Matrix

Als er klassen zijn gedefinieerd om urgentie en impact in te schalen, dan kan een *Incident Prioriteit Matrix* gebruikt worden om prioriteringsklassen te herleiden. In het onderstaande voorbeeld zijn de klassen uitgewerkt met een code en kleuren.

		Impact		
		Hoog	Midden	Laag
Urgentie	Hoog	1	2	3
	Midden	2	3	4
	Laag	3	4	5

Code/kleur	Omschrijving	Reactietijd	Oplossingstijd
1	Kritiek	Onmiddellijk	1 uur
2	Hoog	10 Minuten	4 uur
3	Medium	1 uur	8 uur
4	Laag	4 uur	24 uur
5	Zeer laag	1 dag	1 Week

3.5 Verantwoordelijkheid

De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het College van B&W en/of het bestuur van de ABG-organisatie en namens deze bij de proceseigenaar.

3.6 Proceseigenaar

De proceseigenaar is de CISO.

3.7 Actualiteit

De proceseigenaar is verantwoordelijk voor het actueel houden van deze procedure. Indien de procedure inhoudelijk wijzigt, draagt de proceseigenaar zorg voor communicatie daarover en distributie en archivering van de procedure.

3.8 Uitvoering

1. Elke medewerker van de Organisatie (zowel intern als extern) is verplicht een vermoedelijk beveiligingsincident mondeling of schriftelijk te melden aan de CISO en indien relevant aan de direct leidinggevende of de vertrouwenspersoon. Indien de CISO opmerkt dat het beveiligingsincident (vermoedelijk) nadelige gevolgen heeft of heeft gehad voor persoonsgegevens, behandeld deze het tevens als een datalek en licht hierover de functionaris gegevensbescherming of diens vervanger in.

2. De medewerkers van de Organisatie zijn eveneens verplicht zwakke plekken in de beveiliging (of het vermoeden daarvan) te melden aan de CISO. Een dergelijke verplichting is erop gericht tekortkomingen in de beveiliging zo snel mogelijk te ontdekken en te kunnen oplossen.

3. De medewerkers van de Organisatie zijn eveneens verplicht onvolkomenheden in de programmatuur (of vermoeden daarvan) op het terrein van beveiliging te melden aan de CISO. Een dergelijke verplichting is erop gericht onvolkomenheden in de programmatuur zo snel mogelijk te ontdekken en te kunnen oplossen.

4. Door de CISO wordt het (bijna) incident geregistreerd.

5. Door de CISO wordt vervolgens het (bijna) incident onderzocht als 1e lijns.
   Bij dit onderzoek wordt aandacht besteed aan de volgende aspecten:
   a. Wat is de aard van het (bijna) incident;
   b. welke systemen zijn betrokken;
   c. wat is de oorzaak dat dit (bijna) incident heeft plaatsgevonden;
   d. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
   e. is het (bijna) incident verwijtbaar;
   f. is een eventuele tekortkoming in de beveiliging hersteld;
   g. kan dit (bijna) incident nogmaals optreden;
   h. welke acties moeten worden getroffen om herhaling te voorkomen.

i. Bij dit onderzoek wordt de melder betrokken.

6. Door de CISO wordt vervolgens onmiddellijk de urgentie bepaald van het gemelde incident en deze gebruikt daarvoor de in deze procedure opgenomen urgentietabel. De urgentie wordt geregistreerd. Bij een hoge urgentie wordt meteen contact gezocht met de afdelingsmanager Dienstverlening.

7. Tegelijk wordt door de CISO onmiddellijk de vermoedelijke impact bepaald en deze gebruikt daarvoor de in deze procedure opgenomen impacttabel. De CISO bepaalt in eerste instantie hoeveel tijd en middelen nodig zijn voor afhandeling van het beveiligingsincident.

8. Aan de hand hiervan en de ernst van het incident wordt de prioriteit bepaald. Deze gegevens worden gecombineerd door de CISO volgens de *Incident Prioriteit Matrix*. De CISO draagt er zorg voor dat binnen de gedefinieerde reactietijd wordt gereageerd naar de melder en dat het incident wordt opgelost binnen de aangegeven oplostijd.

9. Ingeval van een mogelijk datalek met betrekking tot persoonsgegevens wordt het incident gemeld aan de functionaris gegevensbescherming en bij diens afwezigheid aan diens vervanger. Zie vervolgens Procedure meldplicht datalekken (blz. 9)
    a. Bij incidenten met de prioriteit hoog of kritiek wordt de afdelingsmanager Dienstverlening ingeschakeld door de CISO. In overleg met het management van de betrokken organisatieonderdelen bepaalt de CISO of een onderzoeksteam samengesteld moet worden.
    b. De CISO neemt tevens direct maatregelen om bewijsmateriaal en andere gegevens die in dit stadium als relevant worden beschouwd, veilig te stellen. De CISO betrekt hierbij tevens het SSC Equalit en de functionaris gegevensbescherming als het om persoonsgegevens gaat.

10. De CISO stelt van het onderzoek een verslag op en rapporteert dit aan de betrokken leidinggevenden. Tevens wordt de melder schriftelijk geïnformeerd over de uitkomsten van het onderzoek.

11. Relevante zaken worden door de CISO intern gemeld aan de Beveiligingscommissie en extern ingeval van *prioriteitsklasse 1 Kritiek* via de landelijke opschaling aan de IBD → NCSC en ingeval van *ernstige* aantasting van de beveiliging van persoonsgegevens aan de Autoriteit Persoonsgegevens. Samen met het team Communicatie wordt bepaald hoe naar het publiek wordt gecommuniceerd.
    a. Ingeval van andere prioriteitsklassen wordt een melding bij IBD door de CISO gedaan indien deze dat nodig acht. Inzet van communicatie is optioneel.
    b. Indien een incident plaatsvindt met betrekking tot de reisdocumenten of rijbewijzen, wordt de burgemeester geïnformeerd.

12. Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De CISO bekijkt periodiek een samenvatting van de informatie. Zowel de meldingen als de wijze van afhandeling worden door de CISO in de managementrapportage opgenomen.

13. In geval van overtreding van de beveiligingsvoorschriften kunnen er door de Organisatie disciplinaire maatregelen getroffen worden. Hierover wordt vooraf altijd de secretaris en de functionaris gegevensbescherming geraadpleegd. De CISO brengt hierover advies uit aan de secretaris. Onder ”disciplinaire maatregelen” wordt verstaan: formele procedures die zijn opgesteld voor (ingehuurde) medewerkers die opzettelijk het beveiligingsbeleid of de beveiligingsprocedures van de Organisatie doorbreken.

14. Voor een eventuele vervolging naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en – na aangifte- te worden gepresenteerd aan het Openbaar Ministerie.

15. Bij (het vermoeden van) een incident is de bewaartermijn van de verzamelde gegevens minimaal drie jaar.

4 Procedure melden van datalekken

4.1 Inleiding

Niet ieder datalek hoeft bij de AP of aan de betrokkene(n) te worden gemeld. Afhankelijk van de impact van het datalek en de kans dat die impact optreedt, wordt bepaald of melding nodig is. In dit document worden handvatten aangereikt om dit per geval te kunnen bepalen.

4.2 Over datalekken

Voorbeelden van datalekken:

- De verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden.
- Per abuis versturen van een e-mail met persoonsgegevens naar de verkeerde ontvanger (Outlook vult e-mailadressen makkelijk aan) en er zijn personen met dezelfde voor- en of achternaam.
- Een medewerkers verliest zijn tas met daarin alle fysieke stukken met persoonsgegevens.
- Een kwijtgeraakte of gestolen USB-stick, laptop of smartphone met daarop toegankelijke bestanden met persoonsgegevens van cliënten voor bijvoorbeeld de WMO of Jeugdzorg.
- Een geprinte lijst met persoonsgegevens die wordt verloren.
- Tijdens het per post verzenden worden per abuis 2 brieven met een zorgbeschikking voor verschillende personen in één envelop gestopt.
- Een webapplicatie heeft grove beveiligingslekken waardoor de kans op misbruik van persoonsgegevens aannemelijk is.
- Een verkeerd bestand wordt geüpload naar een SaaS provider waardoor ongeautoriseerde medewerkers via een webportal inzage krijgen in persoonsgegevens.
- Het versturen van een brief naar een foutief adres kan een datalek zijn indien in de brief persoonsgegevens staan waarvan misbruik zou kunnen worden gemaakt.

Voorwaarden dat er sprake is van een datalek (niet cumulatief):

- De kans is aanwezig dat een onbevoegd persoon de gegevens heeft ingezien en/of gewijzigd;
- gegevens zijn vernietigd of verwijderd, waarbij het niet mogelijk is deze terug te halen;
- er is sprake van een ernstig beveiligingslek waarbij het lek direct toegang geeft tot persoonsgegevens;
- blootstelling heeft geleid (of dat er een aanzienlijke kans op is) tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens of de persoonlijke levenssfeer van betrokkene(n).

  TENZIJ:
- Er kan redelijkerwijs worden uitgesloten dat persoonsgegevens door onbevoegden zijn geraadpleegd of gewijzigd (bijvoorbeeld de persoonsgegevens zijn versleuteld).
- Er kan redelijkerwijs worden uitgesloten dat persoonsgegevens verloren zijn gegaan.

4.3 Uitvoering

4.3.1 Inlichten van de betreffende personen binnen de organisatie

1. Zodra een datalek is opgemerkt door een medewerker van de Organisatie of een van diens (keten)partners dient dit door deze medewerker of via het betreffende afdelingshoofd onverwijld te worden meegedeeld aan de functionaris gegevensbescherming, de CISO of het algemene contactpunt voor vragen over privacy en de bescherming van persoonsgegevens avg@abg.nl (met onderwerp “datalek”).

2. Indien een (keten)partner van de Organisatie optreedt als een verwerker van persoonsgegevens behorende tot de Organisatie en kennis neemt van een datalek m.b.t. deze persoonsgegevens, informeert deze de verwerkingsverantwoordelijke (de Organisatie) hierover zonder onredelijke vertraging. Dit wordt tevens vastgelegd in afspraken die met de verwerker worden gemaakt t.a.v. de omgang met en verwerking van persoonsgegevens.

3. De CISO schakelt in ieder geval de functionaris gegevensbescherming of diens vervanger in als de CISO opmerkt of vermoedt dat het beveiligingsincident (mogelijk) nadelige gevolgen heeft of heeft gehad voor (de bescherming van) persoonsgegevens. De functionaris gegevensbescherming of diens vervanger beoordelen of er daadwerkelijk gesproken kan worden van een inbreuk in verband met persoonsgegevens (datalek).

4.3.2 Documenteren van (interne en externe) meldingen

4. De functionaris gegevensbescherming of diens vervanger documenteert alle inbreuken in verband met persoonsgegevens (datalekken), met inbegrip van de feiten omtrent het datalek, de gevolgen daarvan en de genomen corrigerende maatregelen. Alle benodigde informatie wordt bij de desbetreffende medewerker(s) opgevraagd.
   De registratie van de te melden, gemelde en de niet gemelde datalekken vindt centraal plaats door de functionaris gegevensbescherming of diens vervanger. Hierin worden ook de meldingen geregistreerd die via een of meerdere verwerkers zijn binnengekomen over persoonsgegevens van de Organisatie.
   De documentatie stelt de AP eventueel in staat om de naleving van dit artikel te controleren. (artikel 33 lid 5 AVG)

4.3.3 Melden aan de Autoriteit Persoonsgegevens

5. De functionaris gegevensbescherming of diens vervanger meldt het datalek conform artikel 33 lid 1 AVG bij de AP, indien:
   a. Het gaat om persoonsgegevens;
   b. De Organisatie of een van de onderliggende vier overheidsinstellingen optreedt als verwerkingsverantwoordelijke met betrekking tot een bepaalde verwerking van persoonsgegevens;
   c. Er bij deze verwerking technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd;

d. De AP hanteert sinds 2015 in Beleidsregels t.a.v. de meldplicht van datalekken dat er sprake moet zijn van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Dit speelt als het gaat om persoonsgegevens van gevoelige aard en/of als de aard en omvang van de inbreuk dit aannemelijk maken. De omvang van de inbreuk heeft betrekking op het aantal personen waarvan persoonsgegevens in het geding zijn.

   Let op! Deze beleidsregels golden onder de Wbp. De AVG hanteert een lagere drempel om de autoriteit in te schakelen, namelijk dat er een melding bij de AP gemaakt dient te worden bij ieder risico voor de rechten en vrijheden van de betrokkene. Bij invoering van de AVG kunnen de beleidsregels uit 2015 door het AP worden aangepast, maar dit is vooralsnog niet gebeurd.

6. Indien blijkt dat een gemeld datalek geen melding aan de AP behoeft, wordt door de functionaris gegevensbescherming of diens vervanger de registratie bijgewerkt, wordt een terugkoppeling aan de melder gegeven en wordt de melding gesloten.

7. Als een melding op basis van de beoordeling aan de wettelijke criteria van een datalek voldoet, dan dient deze onverwijld te worden gemeld bij Autoriteit Persoonsgegevens via het Meldloket datalekken Autoriteit Persoonsgegevens. Ga hiervoor naar https://datalekken.autoriteitpersoonsgegevens.nl/.

8. Deze melding dient plaats te vinden zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat de verwerkingsverantwoordelijke er kennis van heeft genomen. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging. (artikel 33 lid 1 AVG)

9. Een melding aan Autoriteit Persoonsgegevens zal in veel gevallen niet in één keer volledig kunnen zijn en kunnen worden afgerond. Daarnaast is het is mogelijk dat na onderzoek de initiële melding wordt ingetrokken. Kortom, altijd direct melden (ook bij twijfel) en daarna de melding zo nodig aanvullen. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie namelijk zonder onredelijke vertraging in stappen worden verstrekt (artikel 33 lid 4 AVG). De functionaris gegevensbescherming of diens vervanger dient na te gaan of en wanneer een melding compleet is.

10. Voor wat betreft de inhoud van de melding, volgt uit artikel 33 lid 3 AVG dat op zijn minst aan de AP wordt meegedeeld of omschreven:
    a. de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de oorzaak van de inbreuk, de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie.

b. de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
c. de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens, zoals (de kans op) identiteitsfraude, financiële schade en schending beroepsgeheim;
d. de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

4.4.4 Melden aan de betrokkene(n)

11. Wanneer de inbreuk in verband met persoonsgegevens (datalek) waarschijnlijk een *hoog* risico inhoudt voor de rechten en vrijheden van natuurlijke personen, informeert de verwerkingsverantwoordelijke de betrokkene(n) onverwijld over het datalek (artikel 34 AVG). Het hoge risico bestaat in ieder geval bij persoonsgegevens met een gevoelige aard.

    Let op! Als de Wet BRP van toepassing is, mag er **geen** melding uitgaan naar de betrokkene(n). Dit is ter bescherming van de belangen van de betrokkene(n). Er mag daarbij zodoende ook geen afweging worden gemaakt voor ieder individueel geval. De Nederlandse overheid gebruikt hierbij de ruimte tot beperking van het recht aan de betrokkene om geïnformeerd te worden (Overweging 73 AVG).

    In andere gevallen, zal het op grond van artikel 41 van de Uitvoeringswet AVG door de functionaris gegevensbescherming of diens vervanger zorgvuldig moeten worden afgewogen of in het concrete geval een uitzondering op de beperking van het recht van de betrokkene gerechtvaardigd is. Deze uitzondering dient alleen plaats te vinden indien dit strikt noodzakelijk is en op proportionele wijze gebeurt. De factoren waar rekening mee dient te worden gehouden, staan opgesomd in artikel 41 lid 2 Uitvoeringswet AVG. Per geval kunnen de relevante factoren worden ingevuld. Zo kan een melding worden uitgesteld, indien een (te vroege) melding het onderzoek naar de oorzaak van de inbreuk kan frustreren.

12. De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld (artikel 34 lid 3 AVG):
    a. de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling of het anonimiseren van data;
    b. de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet zal realiseren;
    c. de mededeling onevenredige inspanningen zou vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

13. De verantwoordelijkheid voor het onderhouden van het contact met de persoon of personen die door het datalek is of zijn getroffen (de betrokkenen), ligt bij de proceseigenaar van het proces waar de gelekte persoonsgegevens worden verwerkt. De proceseigenaar is zodoende verantwoordelijk voor het organiseren en inlichten van de betrokkene(n). Bij afwezigheid van de proceseigenaar wordt de functionaris gegevensbescherming of bij diens vervanger hiermee belast.

14. De mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van het datalek en ten minste de volgende gegevens en maatregelen:
    d. de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
    e. de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
    f. de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.
    g. Indien mogelijk, de maatregelen die de betrokkene zelf zou kunnen treffen om zijn persoonsgegevens te beschermen tegen de gevolgen van de inbreuk.[1]

15. Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan deze daartoe eventueel verplicht worden door de AP nadat deze heeft beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt. De AP kan ook besluiten een van de onder punt 9 bedoelde voorwaarden is voldaan. (artikel 34 lid 4 AVG)

16. Door de functionaris gegevensbescherming of bij diens afwezigheid CISO, wordt een terugkoppeling aan de melder verzorgd namens de proceseigenaar, waarna de melding is afgerond. Uit de registratie kunnen lessen worden geleerd voor toekomstige situaties. De functionaris gegevensbescherming analyseert de meldingen periodiek hierop.

17. Het is de verantwoordelijkheid van de proceseigenaar om **lering** te trekken uit de situatie en maatregelen te treffen om datalekken in vergelijkbare situaties te kunnen voorkomen of in ieder geval de schadelijke gevolgen voor de persoonlijke levenssfeer zoveel mogelijk te beperken.

4.5 Bewaartermijn geregistreerde datalekken

18. Geregistreerde datalekken worden conform de Wbp voorschriften 3 jaar bewaard.

[1] Article 29 Data Protection Working Party, *Guidelines On Personal Data Breach Notification Under Regulation 2016/679 As Last Revised And Adopted On 6 February 2018*, Wp250rev.01, P.30.

4.6 Verantwoordelijkheden

Het college van Burgemeester en Wethouders (college van B&W) is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente.

4.7 Bestuurlijke boete

Als er geen melding wordt gemaakt van een datalek bij de Autoriteit Persoonsgegevens waar dit wel noodzakelijk was, kan dit bestraft worden met een bestuurlijk boete oplopend tot € 820.000,- of 10% van de jaaromzet van de rechtspersoon (alleen na een voorafgaande bindende aanwijzing, tenzij de overtreding opzettelijk is begaan of een gevolg is van ernstig verwijtbare nalatigheid).[2]

[2] Boetebeleidsregels Autoriteit Persoonsgegevens 2016.

5 Bijlage Beslissingsschema datalekken

Bij de beslissing of een gebeurtenis moet worden gemeld aan de Autoriteit Persoonsgegevens en eventueel daarnaast ook aan de betrokkene, horen er een aantal afwegingen gemaakt de worden. Het onderstaande schema geeft schematisch weer wat eerder in dit document is besproken.

Aldus vastgesteld door burgemeester en wethouders van gemeente Alphen-Chaam,
d.d.

mr. M.M. Hendrickx
secretaris

mr. J.W.M.S. Minses
burgemeester

Aldus vastgesteld door burgemeester en wethouders van gemeente Baarle-Nassau,
d.d.

Ir. J.C. Slagboom
secretaris

M.H.M.R. de Hoon-Veelenturf
burgemeester

Aldus vastgesteld door burgemeester en wethouders van gemeente Gilze en Rijen,
d.d.

drs. R. Wiersema
secretaris

dr. A.J.W. Boelhouwer
burgemeester

Aldus vastgesteld door het bestuur van de ABG-organisatie,
d.d.

drs. R. Wiersema
algemeen directeur

dr. A.J.W. Boelhouwer
voorzitter