Privacybeleid NOARDEAST-FRYSLÂN

Vastgesteld door burgemeester en wethouders op 3 november 2020

1. Inleiding

1.1 Algemeen

Iedereen heeft recht op privacy. Gemeenten verzamelen en gebruiken veel persoonsgegevens. Deze gegevens zijn nodig voor het uitvoeren van taken. De gemeente is verantwoordelijk voor de bescherming van deze persoonsgegevens.

De bescherming van persoonsgegevens speelt een steeds belangrijker rol door de:

- technologie die zich steeds sneller ontwikkelt;
- toename in dataverkeer;
- toename in het verzamelen en delen van gegevens;
- risico's van cybercrime;
- samenleving die steeds kritischer wordt;
- rechten van inwoners om inzicht te verkrijgen in de verwerking van hun
- persoonsgegevens;
- toename van de hoeveelheid gevoelige informatie van personen (bijvoorbeeld jeugdzorg, maatschappelijke ondersteuning, de zorg voor chronisch zieken, ouderen en gehandicapten, leerling zaken.)

Iedereen heeft recht op correcte, veilige en betrouwbare informatieverwerking en moet erop kunnen vertrouwen dat de gemeente zorgvuldig met deze gegevens omgaat.

1.2 Reikwijdte en afbakening privacy

Het gemeentelijk privacybeleid is - naast informatiebeveiliging - onderdeel van het overkoepelende begrip informatieveiligheid en is van toepassing op alle taken en processen waar de gemeente , respectievelijk de burgemeester, voor verantwoordelijk is. Het privacybeleid heeft betrekking op de bescherming van persoonsgegevens van personen van wie de gemeente Dongeradeel gegevens verwerkt (of laat verwerken).

Onder persoonsgegevens verstaan we alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Dit betekent dat informatie direct over iemand gaat of naar deze persoon te herleiden is.

Er is al snel sprake van 'verwerken' van persoonsgegevens. Verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen van gegevens valt allemaal onder het verwerken van persoonsgegevens.

Verdere definities met betrekking tot de verwerking van persoonsgegevens zijn opgenomen in de Algemene Verordening Gegevensbescherming (AVG)

1.3 Scope

Het privacybeleid is van toepassing op:

- Alle (werk-)processen waarbinnen persoonsgegevens worden verwerkt;
- Informatiesystemen waarin persoonsgegevens worden verwerkt, waarvoor de gemeente (intern en extern) verantwoordelijk is;
- Alle ruimten en devices die door bestuurders en gemeenteambtenaren intern en extern worden gebruikt waar (op) persoonsgegevens worden verwerkt;
- Alle geldende normen en regels op het gebied van privacy.

1.4 Opbouw privacybeleid

Het privacybeleid geldt als algemeen beleid. Hierin zijn de kaders met de risico's en maatregelen beschreven om te voldoen aan wet- en regelgeving. Voor bepaalde domeinen kan het nodig zijn om aanvullend specifiek privacybeleid vast te stellen.

De organisatie van verantwoordelijkheden, functies en rollen waarmee de gegevensbescherming in de gemeente Noardeast-Fryslân wordt geborgd, is opgenomen in het Strategisch Informatieveiligheidbeleid.

1.5 Wetten en regels

De juridische grondslag voor privacy is terug te vinden in wet- en regelgeving. De bescherming van de privacy bij de verwerking van persoonsgegevens is een grondrecht. Dit is geregeld in:

- Grondwet (art. 10)
- Handvest van de grondrechten van de Europese Unie (EHRM)
- Europees Verdrag voor de Rechten van de Mens (EVRM)
- Internationaal Kinderrechtenverdrag (IVRK)

De Europese Algemene Verordening Gegevensbescherming (AVG) is op 25 mei 2018 in werking getreden en is een EU-verordening die rechtstreekse werking in de lidstaten heeft. Vanaf die datum moet iedere organisatie die persoonsgegevens verwerkt voldoen aan de eisen van de AVG.

Verder is ook in specifieke regelgeving invulling gegeven aan de bescherming van de privacy bij de verwerking van persoonsgegevens zoals in de Wet maatschappelijke ondersteuning (WMO 2015), de Jeugdwet en de Wet Basisregistratie Personen (Brp).

Informatiebeveiliging en de bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens. In het Strategisch informatiebeveiligingsbeleid zijn maatregelen opgenomen om de gegevens te beschermen.

Het privacybeleid omvat de gehele ‘data life cycle’; van het genereren of verzamelen van gegevens, het dagelijks gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan. Er wordt geen onderscheid gemaakt tussen papieren of digitale informatieverwerking.

2. Privacybeleid

2.1. Doelstelling

Doel van dit privacybeleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen waarvan de gemeente Noardeast-Fryslân persoonsgegevens verwerkt. Het privacybeleid draagt bij aan:

- het beschermen van de privacy van personen van wie de gemeente Noardeast-Fryslân gegevens verwerkt of laat verwerken;
- maatschappelijk vertrouwen en draagvlak;
- beheersen van gemeentelijke afbreuk- en aansprakelijkheidsrisico’s;
- het met vertrouwen verantwoording af kunnen leggen aan de gemeenteraad, waar nodig de Autoriteit Persoonsgegevens (AP) of de rechter;
- het in kunnen spelen op wettelijke en technologische ontwikkelingen.

2.2. Uitgangspunten

Iedereen werkzaam binnen de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen. Het is belangrijk om persoonsgegevens rechtmatig, behoorlijk en transparant te verwerken[1]. De uitgangspunten hierbij zijn:

- betrokkene heeft toestemming gegeven voor de verwerking of de verwerking is noodzakelijk:
    - op basis van de wet of een overeenkomst;
    - ter bescherming van vitale belangen;
    - voor een taak in het algemeen belang of voor de uitoefening van een publieke taak;
- betrokkene is vooraf in eenvoudige en duidelijke taal geïnformeerd dat zijn/haar persoonsgegevens worden verwerkt en voor welk doel;
- alleen persoonsgegevens die noodzakelijk zijn voor het doel worden verwerkt;
- persoonsgegevens zijn correct en actueel;
- verzoeken van betrokkene op het gebied van rechten zoals, ‘recht op inzage’ , ‘recht op rectificatie’ ‘het recht om vergeten te worden’ worden opgevolgd overeenkomstig de wettelijke voorwaarden (o.a. na toereikende identificatie);
- als registratie niet meer noodzakelijk is voor het doel, dan moeten de persoonsgegevens worden verwijderd of geanonimiseerd;
- persoonsgegevens zijn beveiligd door middel van technische en organisatorische maatregelen;
- zorg voor privacy is evenals beveiliging een kwaliteitsaspect en maakt deel uit van de integrale verantwoordelijkheid van het lijnmanagement.

[1] artikel 5 AVG e.v. ‘Beginselen betreffende verwerking van persoonsgegevens’

Het college van B&W, respectievelijk de burgemeester, is verantwoordelijk voor het naleven van deze uitgangspunten en moet dit bij de toezichthouder (AP) kunnen (laten) aantonen.

2.3 Risico's

Bij schending van de privacy is het college van B&W, respectievelijk de burgemeester, wettelijk aansprakelijk. Het verwijtbaar onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving kan leiden tot:

- het betalen van schadevergoeding. Elke benadeelde heeft hier recht op;
- reputatieschade en herstelkosten. Deze kunnen fors zijn en leiden tot verlies van vertrouwen in de overheid;
- onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding van de AVG kan de Autoriteit Persoonsgegevens, de landelijk toezichthouder, een (hoge!) boete opleggen.

Binnen bepaalde domeinen wordt er gewerkt met zeer gevoelige bijzondere persoonsgegevens zoals medische gegevens, gegevens over iemands financiële situatie of strafrechtelijke gegevens. Voorbeelden zijn met name te vinden in het sociaal domein, leerlingzaken, burgerzaken. Aan de verwerking van deze persoonsgegevens zijn aanvullende voorwaarden gesteld[2]. De risico's bij de verwerking van bijzondere persoonsgegevens zijn hoger.

De risico's van schending van de privacy voor personen variëren van ongemak, substantiële benadeling, stigmatisering, uitsluiting of gevaren voor de gezondheid en de persoonlijke veiligheid.

Om de risico's te beperken moeten maatregelen worden getroffen. Deze maatregelen zijn beschreven in hoofdstuk 4. Leidend daarbij is dat privacy-eisen zoveel mogelijk worden geïntegreerd in regulier en/of al bestaand (domein) beleid en vertaald naar processtappen die worden geïntegreerd in het reguliere werkproces.

2.4 Evaluatie

Het privacybeleid wordt eens per twee jaar geëvalueerd. Indien daartoe aanleiding bestaat wordt het privacybeleid (eerder) bijgesteld.

3. Taken en verantwoordelijkheden

3.1. Doelstelling

De bescherming van de privacy van betrokkene(n) beleggen bij de verantwoordelijke functionarissen.

3.2. Afbakening rollen en verantwoordelijkheden

Omdat informatiebeveiliging een randvoorwaarde vormt voor privacybescherming, moeten de taken en verantwoordelijkheden ten aanzien van beide disciplines op elkaar zijn afgestemd. Het Strategisch Informatieveiligheidsbeleid bevat een volledige beschrijving van de overlegstructuur en de taken, bevoegdheden, verantwoordelijkheden van alle medewerkers met een specifieke rol ten aanzien van informatieveiligheid.
Nogmaals, onder informatieveiligheid wordt naast informatiebeveiliging ook de bescherming van persoonsgegevens (privacy) begrepen.
In dit hoofdstuk wordt onderstaande RASCI-tabel uitgewerkt, waarin de belegging van rollen en verantwoordelijkheden op organisatieniveau is opgenomen.

Het college van B&W is eindverantwoordelijk, maar iedereen binnen de organisatie is verantwoordelijk voor de informatieveiligheid en dus het waarborgen van privacy.
Onderstaande tabel brengt op hoofdlijnen de verantwoordelijkheden in beeld:

	Verantwoordelijk	Rol
R	Responsible / feitelijk verantwoordelijk	Directie Afdelingsmanagers Teamleiders Alle medewerkers (inclusief inhuur/externen)

[2] art. 9, art. 10 AVG 'verwerking van bijzondere persoonsgegevens'

A	Accountable / eindverantwoordelijk	College van B&W
S	Supporting / uitvoerend	Managers Teamleiders Alle medewerkers (inclusief inhuur/externen)
C	Consulted / adviserend	Kernteam informatieveiligheid
I	Informed / geïnformeerd	Gemeenteraad[3] Belanghebbenden / betrokkenen

3.2.1 Het college van B&W, respectievelijk de Burgemeester:

- is bestuurlijk integraal eindverantwoordelijk voor de informatieveiligheid;
- rapporteert aan de gemeenteraad over de uitvoering van het beleid;
- stelt twee jaarlijks het werkprogramma privacybeleidsvoering vast, mede op basis van rapportage van de FG en de aanbevelingen die hij hierin doet;

Binnen het college is een collegelid portefeuillehouder informatieveiligheid.

3.2.2 De directie

- de directie DDFK-organisatie is ambtelijk verantwoordelijk voor risicomanagement, implementatie en naleving van beleidsregels informatieveiligheid.
- stelt vanuit informatieveiligheid kaders vast voor de bescherming van privacy overeenkomstig wet- en regelgeving;
- stelt het wettelijk voorgeschreven Register van Verwerkingen vast. In dit Register staan alle werkprocessen waarbij persoonsgegevens worden verwerkt. Aan elk werkproces is functioneel een proceseigenaar toegekend.
- is transparant over de beleidsvoering informatieveiligheid en voert op dit thema evenwichtig communicatiebeleid waarbij proceseigenaren zo nodig voorzien in bijzondere voorlichting aan specifieke doelgroepen.

1. Hieruit volgt dat de directie er op stuurt dat:
a.) binnen een (werk-)proces alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het realiseren van het procesdoel;
b.) bij (werk-)processen waaraan privacy-risico's zijn verbonden, de proceseigenaar een procesplan en een privacy impact assessment (PIA) hanteert. Het te hanteren model hiervoor is nader uitgewerkt in de 'Werkinstructie PIA' van VNG-Realisatie;
c.) een PIA duidelijk en actueel is, overeen stemt met de werkelijkheid en periodiek wordt geëvalueerd;
d.) een proceseigenaar, als onderdeel van zijn verantwoordelijkheden, regie voert en toezicht houdt op zijn proces(sen) op basis van de privacy-beleidskaders;
e.) bij privacy-incidenten de proceseigenaar de incidentenprocedure hanteert zoals vastgelegd in het besluit "Organisatie informatieveiligheid DDFK-organisatie" en in het besluit "Procedure beveiligingsincident en meldplicht datalek";
f.) bij risicovolle procesvoering de proceseigenaar periodiek een audit laat uitvoeren tegen deze privacy-beleidskaders en zijn PIA;
g.) gecontroleerd wordt of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkene(-n) te beschermen;
h.) dat documentatie van beleid en maatregelen plaatsvindt zodat op ieder moment maatschappelijk en juridisch uitleg kan worden gegeven over de deugdelijkheid van de aanpak;
i.) eens per twee jaar het privacybeleid op basis van de evaluatie en aanpassingen wordt beoordeeld;
j.) in een team van professionals, het kernteam Informatieveiligheid (zie 3.2.5), is voorzien dat de directie en management ondersteunt in de uitvoering van het privacybeleid;
k.) de FG en de CISO naar behoren en tijdig worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
l.) voorzien wordt in faciliteiten voor bewustwording en training;

m.) het privacybeleid wordt gehandhaafd. De gemeente Noardeast-Fryslân heeft een FG aangesteld die toeziet op de borging van privacy in de gemeentelijke organisatie;
Binnen de directie is de adjunct-directeur portefeuillehouder Informatieveiligheid.

[3] De gemeenteraad heeft privacyrechtelijk geen controlerende taak maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak.

3.2.3 Managers (MT-ers) en Teamleiders

Vanuit de lijnverantwoordelijkheid is de teamleider - onder verantwoordelijkheid van de integraal manager - verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar team plaatsvindt. Daarbij ontvangt deze ondersteuning van de beheerder informatieveiligheid van de afdeling / het team.

De teamleider:
1. zorgt voor naleving van AVG-wet- en regelgeving en het privacybeleid (zoals rechtmatige, behoorlijke en transparante verwerking, geeft uitvoering aan rechten van betrokkenen, gebruikt en evalueert PIA's, past 'Privacy by design/default' toe in werkprocessen, zorgt voor registratie van verwerkingsactiviteiten, creëert privacybewustzijn etc.)
2. zorgt er voor dat de beheerder informatieveiligheid naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
3. meldt aan de beheerder informatieveiligheid een nieuwe, een wijziging in of een beëindiging van een verwerking van persoonsgegevens ten behoeve van het Register van Verwerkingen;
4. stelt informatieveiligheid en daarmee privacy regulier aan de orde in het werkoverleg;
5. zorgt dat er binnen het team één of meer beheerders Informatieveiligheid(s) zijn die als aanspreekpunt voor informatieveiligheid optreden.

3.2.4 Medewerkers

Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkene(n). Dat betekent dat iedereen gebonden is aan een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.

3.2.5 Kernteam Informatieveiligheid

Het Kernteam informatieveiligheid bestaat minimaal uit de Chief Information Security Officer (CISO), de Functionaris Gegevensbescherming (FG), de Informatie-manager, de Informatiearchitect/ Gegevensregisseur en een Communicatieconsulent . Dit team wordt waar nodig uitgebreid met de betrokken afdelingsmanager, teamleider of een taakspecialist (bijv. juridische zaken). E.e.a. staat uitgebreid beschreven in bijlage 1, "Organisatie informatieveiligheid DDFK-organisatie".
Belangrijkste taak van dit kernteam is advies uit te brengen en op te treden bij een incident in de informatiebeveiliging waaronder een datalek.

3.2.6 Functionaris Gegevensbescherming (FG)

Een FG wordt wettelijk aangesteld op grond van artikel 37 van de Algemene Verordening Gegevensbescherming (AVG).
Wettelijke uitgangspunten o.g.v. art. 38 AVG:
De FG:
1. wordt tijdig en naar behoren geconsulteerd bij alle zaken die verband houden met de bescherming van persoonsgegevens;
2. heeft toegang tot alle persoonsgegevens in de organisatie en de verwerkingsactiviteiten daarvan;
3. is onafhankelijk toezichthouder op de toepassing van de AVG en krijgt geen instructies over de uitvoering van zijn taken;
4. is verplicht tot geheimhouding en vertrouwelijkheid.
5. betrokkenen kunnen contact met de FG opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van de AVG.

De FG heeft op grond van art. 39 AVG minimaal de volgende taken en bevoegdheden:
1. informeert en adviseert over de verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens;
2. ziet toe op de naleving van wet- en regelgeving en het door het college van B&W vastgesteld beleid met betrekking tot de bescherming van persoonsgegevens;
3. ziet toe op het toewijzen van verantwoordelijkheden, bewustmaking en opleiding van de organisatie op het gebied van de bescherming van persoonsgegevens;
4. geeft advies over Privacy Impact Analyses (PIA);
5. past risicomanagement toe bij de uitvoering van zijn taken;
6. werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens (AP).
Daarnaast heeft de FG een coördinerende taak in het kader van datalekken, is hij meldingsbevoegd voor het melden van een datalek bij de Autoriteit Persoonsgegevens en is hij verantwoordelijk voor het (laten) inrichten en (laten) bijhouden van het Register van Verwerkingsactiviteiten.

De AVG schrijft voor dat de FG rechtstreeks verslag van zijn werkzaamheden uitbrengt aan de hoogste leidinggevende (de directie) en /of aan de Verwerkingsverantwoordelijke (het college van B&W respectievelijk de burgemeester.)

3.2.7 Beheerder Informatieveiligheid

De taken die in de AVG niet (expliciet) zijn belegd bij de FG, zijn onderdeel van het takenpakket van de Beheerder Informatieveiligheid. Belangrijke taak hierbij is dat de Beheerder Informatieveiligheid het Register van Verwerkingen voor zijn / haar afdeling muteert en hiervan melding maakt aan de FG bij wie de centrale toezichtstaak van dit Register is belegd. Daarnaast:
1. stelt zo nodig voor zijn of haar organisatieonderdeel specifiek privacybeleid op, consulteert hierbij de FG en legt het ter vaststelling voor aan de directie;
2. Ondersteunt en wordt geconsulteerd bij de uitvoering van PIA's
3. evalueert, in samenspraak met de FG, het specifiek privacybeleid en doet voorstellen tot implementatie en aanpassingen van dat privacybeleid.

4. Maatregelen

4.1 Doelstelling

Met de maatregelen beschreven in dit hoofdstuk kunnen de doelstellingen van het privacybeleid worden gehaald en de risico's worden beperkt.

4.2 Maatregelen

Onderstaande maatregelen zijn getroffen om persoonsgegevens rechtmatig, behoorlijk en transparant te kunnen verwerken, volgens geldende wet- en regelgeving.

4.2.1 Transparantie:

Betrokkene(n) krijgen vooraf duidelijke informatie (via de website en de dienstverlening (telefonisch, schriftelijk, email)) over de verwerking van hun persoonsgegevens en het doel van de verwerking.

4.2.2 Naleving van het informatiebeveiligingsbeleid:

Op basis van het informatiebeveiligingsbeleid zijn maatregelen getroffen om de bescherming van persoonsgegevens te waarborgen. Informatiebeveiliging is een eerste voorwaarde voor gegevensbescherming in het kader van privacy.

4.2.3 Bewustwording en communicatie:

Bewustwording is essentieel voor het borgen van privacy in de organisatie. Het is belangrijk dat iedereen die werkt met privacygevoelige informatie zich bewust is van het belang om hier zorgvuldig mee om te gaan. Doorlopend wordt er aandacht geschonken aan de bewustwording via het werkoverleg en trainingen.

4.2.4 Register van Verwerkingsactiviteiten:

Er wordt een register bijgehouden met alle verwerkingsactiviteiten van persoonsgegevens per proces. Hierin worden onder andere de doeleinden van de verwerking, categorieën van betrokkene(n) en persoonsgegevens, derden ontvangers, bewaartermijn en maatregelen opgenomen.

4.2.5 Privacy Impact Analyses (PIA's):

Voor (nieuwe en veranderende) processen, diensten en producten en informatiesystemen, waarin persoonsgegevens worden verwerkt, worden PIA's uitgevoerd. Systematisch worden verwerkingen van persoonsgegevens, doeleinden, risico's en (voorgenomen) maatregelen beschreven. Het doel is om de impact van de verwerking op de bescherming van persoonsgegevens in kaart te brengen en uiteindelijk de impact op de betrokkene en de organisatie. Per PIA wordt de FG geconsulteerd.

Als uit een PIA blijkt dat er sprake is van risicovolle verwerkingen wordt de Autoriteit Persoonsgegevens op de hoogte gesteld. Op basis van de uitkomsten van de PIA wordt bepaald met welke frequentie en diepgang audits moeten worden uitgevoerd, welke maatregelen moeten worden genomen en in hoeverre goedkeuring door de FG is vereist.

De wijze waarop een PIA wordt uitgevoerd en wat de vervolgacties op basis van de uitkomsten moeten zijn, wordt - zoals eerder aangegeven - uitgewerkt aan de hand van het model 'Werkinstructie PIA' van VNG-Realisatie.

4.2.6 Privacy by design of privacy by default:

Privacy by design houdt in dat al vanaf het eerste ontwerp van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over:

- het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens;
- gegevensminimalisatie, anonimisering en pseudonimisering;
- de maatregelen die hiervoor nodig zijn.

Privacy by default betekent dat de standaard instellingen in systemen zijn ingesteld om maximale privacy bescherming te borgen. De AVG noemt dit 'Gegevensbescherming door ontwerp en standaardinstellingen'.

4.2.7 Verwerkersovereenkomst:

Een verwerkingsovereenkomst is wettelijk verplicht als het verwerken van persoonsgegevens aan een andere partij, een Verwerker, wordt uitbesteed. Er worden bijvoorbeeld afspraken gemaakt over:

- de doeleinden waarvoor de gegevens mogen worden verwerkt;
- hoe de verwerker met de persoonsgegevens moet omgaan;
- welke beveiligingsmaatregelen moeten worden genomen;
- welke vormen van toezicht de eigenaar van de gegevens uitoefent;
- de geheimhoudingsplicht;
- inschakeling van derden en onderaannemers;
- locatie van de data;
- de rolverdeling bij de afhandeling van datalekken en de uitoefening van rechten van betrokkenen;
- aansprakelijkheid in geval van schade door het niet naleven van regelgeving.

In beginsel wordt het model Verwerkersovereenkomst van de Informatie Beveiligingsdienst (IBD; model VNG-Realisatie) als uitgangspunt genomen.

4.2.8 Meldplicht Datalekken

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. We spreken ook van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 33 AVG).
Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. De meldplicht datalekken regelt wanneer een datalek moet worden gemeld bij de Autoriteit Persoonsgegevens. Een datalek moet aan de betrokkene(n) worden gemeld als de inbreuk waarschijnlijk ongunstige gevolgen heeft voor zijn of haar privéleven. Voor de werkwijze bij een datalek en de rolverdeling wordt verwezen naar het besluit "Procedure beveiligingsincident en meldplicht datalek". (Bijlage 2)

4.2.9 Audits

Vragen, klachten en het incident management zijn vormen van steekproefsgewijze toetsing van de privacybeleidsvoering. Om niet voor verrassingen te worden geplaatst, is het zaak dat proceseigenaren ook zelf periodiek (laten) controleren in hoeverre beleidsvoering en feitelijke situatie met elkaar overeenstemmen aan de hand van privacy audits op de gehanteerde ijkpunten.
Op basis van de uitkomsten van de PIA wordt bepaald naar welke zwaarte de audits moeten plaatsvinden. Hierbij worden de volgende typen onderscheiden:

- Quick scan is een beknopte toets onder de verantwoordelijkheid van de proceseigenaar .
- Zelfevaluatie is een uitgebreidere toets onder de verantwoordelijkheid van de proceseigenaar .
- Externe audit is een audit die de proceseigenaar organiseert in samenwerking met de FG en waarbij eventueel een professionele auditor wordt betrokken.

Wanneer een audit plaatsvindt, wordt de FG vanaf het begin betrokken in het audittraject en is hij medeontvanger van het auditrapport.