Privacybeleid

gemeente Súdwest-Fryslân 2018-2020

April 2018

1.1 Algemeen

Het recht op privacy wordt omschreven als het recht *om met rust te worden gelaten*. De Van Dale omschrijft privacy als de persoonlijke vrijheid, het ongehinderd, alleen, in eigen kring of met een partner ergens kunnen vertoeven; gelegenheid om zich af te zonderen, om storende invloeden van de buitenwereld te ontgaan, een toestand waarin een mens er zeker van is dat zonder zijn toestemming zo weinig mogelijk andere mensen zich op zijn terrein zullen begeven. Later is dit uitgebreid met: zelf bepalen wie welke informatie over ons krijgt. Deze nota gaat over dit laatste aspect: de bescherming van de persoonsgegevens. Het recht op privacy is een grondrecht dat is opgenomen in de Grondwet en in diverse internationale verdragen. In de privacywetgeving staat de eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens centraal.

Privacy is een ruim begrip: het gaat om de bescherming van persoonsgegevens, de bescherming van het eigen lichaam en van de eigen woning, de bescherming van familie- en gezinsleven en het recht vertrouwelijk te communiceren via brief, telefoon, e-mail. De belangen van een organisatie om persoonsgegevens te verwerken zijn in beginsel ondergeschikt aan het belang van de persoon zelf. Dit zorgt ervoor dat organisaties die persoonsgegevens verwerken, en dus inbreuk maken op het recht op privacy, zich goed bewust dienen te zijn van de belangen van een goede verwerking en de beveiliging van de persoonsgegevens (gegevensbescherming).

Het belang van goede omgang met persoonsgegevens en de bescherming hiervan ligt in de steeds verdere toename van de digitalisering. In onze informatiemaatschappij brengt dat de bescherming van persoonsgegevens op subtiele wijze onder druk. De belangen van goede gegevensbescherming wordt naast de toename van digitalisering ook belangrijker door:

- technologie die zich zeer snel ontwikkelt;
- toename in dataverkeer;
- toename in het verzamelen en delen van gegevens en de mogelijkheden daarvoor;
- risico's van cybercrime;
- toename van de hoeveelheid gevoelige informatie van personen in systemen (bijvoorbeeld jeugdzorg, maatschappelijke ondersteuning, de zorg voor chronisch zieken, ouderen en gehandicapten, leerling zaken.)

De gemeente Súdwest-Fryslân verwerkt persoonsgegevens. Deze gegevens zijn nodig voor het uitvoeren van de gemeentelijke wettelijke taken van de gemeente. De gemeente Súdwest-Fryslân is verantwoordelijk voor het beschermen van deze persoonsgegevens en vindt het belangrijk dat er zorgvuldig wordt omgegaan met de gegevens van burgers en medewerkers. De gemeente is zich hiervan bewust en zorgt dat de privacy gewaarborgd is, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole. Iedereen heeft namelijk recht op correcte, veilige en zorgvuldige informatieverwerking en moet erop kunnen vertrouwen dat de gemeente zorgvuldig met de persoonsgegevens omgaat. Het hier beschreven privacybeleid geeft daarvoor, naast de geldende wet- en regelgeving, de basis.

1.2 Reikwijdte en afbakening privacy

Het privacybeleid van de gemeente Súdwest-Fryslân is van toepassing op de gehele organisatie, alle taken en processen, onderdelen, objecten en gegevensverzamelingen waar de gemeente voor verantwoordelijk is. Bij uitbesteding aan derden, zoals ICT-leveranciers, zorgaanbieders of gemeentelijke samenwerkingsverbanden, blijft het college van B&W verantwoordelijk voor de goede uitvoering van die taken en voor de zorgvuldige verwerking van persoonsgegevens. Dat betekent dat wanneer er sprake is van het verwerken van persoonsgegevens door een derde partij voorafgaand aan de verwerking schriftelijke afspraken moeten worden gemaakt die voldoen aan de privacyregelgeving. Privacybeleid heeft betrekking op de persoonsgegevens van personen van wie de gemeente gegevens verwerkt (of laat verwerken) en 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.

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 Informatieveiligheidsbeleid 2018-2021 van de gemeente Súdwest-Fryslân zijn de kaders, uitgangspunten en verantwoordelijkheden vastgelegd om informatiebeveiliging structureel te borgen binnen de gemeentelijke organisatie.
Binnen Súdwest-Fryslân hebben we daarnaast het Integriteitsbeleid dat raakt aan het privacybeleid. Informatiebeveiliging, integriteit en het privacy worden vanuit voornoemde samenhang op sommige onderdelen gezamenlijk opgepakt.

1.3 Scope

Het privacybeleid geldt voor:

- alle medewerkers, en externen die zijn ingehuurd, van de gemeente Súdwest-Fryslân;
- alle processen waarbinnen persoonsgegevens worden verwerkt;
- informatiesystemen waarin persoonsgegevens worden verwerkt, waarvoor de gemeente (intern en extern) verantwoordelijk is;
- alle ruimten en devices die intern en extern worden gebruikt waar (op) persoonsgegevens worden verwerkt.

1.4 Opbouw privacybeleid

Het privacybeleid geldt als algemeen breed gemeentelijk 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 of wenselijk zijn om aanvullend specifiek privacybeleid vast te stellen. Hoofdstuk 2 werkt het beleid verder uit.

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:

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

De belangrijkste wet die op dit moment invulling geeft aan de bescherming van privacy van personen bij de verwerking van persoonsgegevens is de Europese Algemene Verordening Gegevensbescherming (AVG). Deze is vastgesteld op 25 mei 2016 en vanaf 25 mei 2018 moeten alle organisaties en overheden in heel Europa hieraan voldoen. De Wet bescherming persoonsgegevens (Wbp) vervalt per die datum.

Verder is ook in specifieke regelgeving invulling gegeven aan de bescherming van de persoonsgegevens zoals in de:

- Wet maatschappelijke ondersteuning (Wmo)
- Jeugdwet
- Wet Basisregistratie Personen (Brp)
- Participatiewet
- Wet algemene bepalingen Burgerservicenummer
- Wet gemeentelijke schuldhulpverlening
- Uitvoeringswet Algemene Verordening gegevensbescherming

Enkele kernbegrippen als het gaat om het verwerken van persoonsgegevens:

Persoonsgegevens
Onder persoonsgegevens verstaan we alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”). Het zijn alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen(art. 4 lid 1 AVG) . Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals iemand gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld: naam, adres, geboortedatum, kenteken). Naast *gewone* persoonsgegevens kent de wet ook *bijzondere* persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, financiële gegevens, medische gegevens en het Burgerservicenummer (BSN). Voor het verwerken van bijzondere persoonsgegevens gelden strenge regels.

Verwerken
Er is al snel sprake van het ‘verwerken’ (art. 4 lid 2 AVG) van persoonsgegevens. Verzamelen, vastleggen, inzien, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, samenbrengen, met elkaar in verband brengen, afschermen, wissen of

vernietigen van gegevens valt allemaal onder het verwerken van persoonsgegevens. Bij elke verwerking van persoonsgegevens is de privacyregelgeving van toepassing.

Gronden voor verwerking
Er moet een grond zijn om persoonsgegevens te kunnen en mogen verwerken. De belangrijkste grond voor de verwerking bij de gemeente is dat de verwerking nodig is 'voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen' (art. 6 AVG). Daarnaast kennen we, als gemeente, de grondslag 'ondubbelzinnige toestemming' afgegeven door de betrokkene waardoor de gemeente gegevens kan verwerken.

Doelbinding
Een basisprincipe uit het privacyrecht is de zogenaamde doelbinding (art. 5 lid sub b). Als persoonsgegevens worden verwerkt, gebeurt dat voor een duidelijk omschreven en gerechtvaardigd doel. De gegevens mogen niet voor een ander doel gebruikt worden. Dat is voor een gemeente, waar veel gegevens worden verwerkt voor verschillende doeleinden, heel belangrijk. Gegevens die bijvoorbeeld nodig zijn voor het verstrekken van een uitkering mogen niet worden gebruikt voor het beoordelen van een vergunning. Als je gegevens wilt gebruiken voor een ander doel dan waarvoor ze in eerste instantie zijn gegeven, dan is ondubbelzinnige toestemming van de betrokkene nodig. Bovendien moeten gegevens worden verwijderd op het moment dat ze niet meer nodig zijn voor het specifieke doel.

Autoriteit Persoonsgegevens (AP)
De instantie die in Nederland toezicht houdt op de naleving van de AVG en andere privacyregelgeving is de Autoriteit Persoonsgegevens (AP).

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

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 persoonsgegevens verwerkt.

Het privacybeleid draagt bij aan:

- het beschermen van de privacy van personen van wie de gemeente gegevens verwerkt of laat verwerken;
- maatschappelijk vertrouwen en draagvlak;
- beheersen van afbreuk- en aansprakelijkheidsrisico's;
- het met vertrouwen verantwoording af kunnen leggen aan het College van B&W, 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 (art. 5 AVG e.v. ' beginselen betreffende verwerking van persoonsgegevens').

De uitgangspunten zijn:

- verwerken van persoonsgegevens gebeurd op basis van vastgestelde wettelijke grondslagen;
- dataminimalisatie: er worden alleen die gegevens uitgewisseld die voor het bereiken van het doel noodzakelijk zijn;
- persoonsgegevens worden niet langer bewaard dan voor het doel waarvoor zij verzameld zijn noodzakelijk is;
- persoonsgegevens worden niet verwerkt anders dan voor het doel waarvoor zij zijn verkregen;
- de gegevens worden niet gebruikt voor doeleinden die onverenigbaar zijn met (of niet herleidbaar zijn tot) het oorspronkelijke doel waarvoor de gegevens nodig zijn;
- indien nodig wordt er toestemming gevraagd voor de verwerking van persoonsgegevens;
- betrokkene is vooraf in eenvoudige en duidelijke taal geïnformeerd dat zijn/haar persoonsgegevens worden verwerkt en voor welk doel=transparantie;
- persoonsgegevens zijn correct en actueel;
- verzoeken van betrokkene op het gebied van rechten zoals 'het recht om vergeten te worden' , 'recht op inzage' , 'recht op rectificatie' worden opgevolgd overeenkomstig de wettelijke voorwaarden;

- 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.

Het college van B&W is verantwoordelijk voor het naleven van deze uitgangspunten en moet te allen tijde kunnen aantonen dat zij aan de wet- en regelgeving voldoen.

2.3 Risico's

Bij schending van de privacy is de gemeente aansprakelijk. Het verwijtbaar onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving kan leiden tot:

- reputatieschade en imagoverlies. Deze kunnen fors zijn en leiden tot verlies van vertrouwen in de gemeente Súdwest-Fryslân en in de overheid in het algemeen;

- onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding van de AVG of andere wet- en regelgeving op het gebied van privacy kan de Autoriteit Persoonsgegevens, de landelijk toezichthouder, een boete opleggen. Onder de AVG kunnen de boetes oplopen tot maximaal € 20 miljoen;

- het betalen van schadevergoeding aan gedupeerden.

Binnen bepaalde domeinen wordt er gewerkt met zeer gevoelige bijzondere persoonsgegevens zoals medische gegevens, gegevens over iemands financiële situatie of strafrechtelijke gegevens. Voorbeelden zijn het sociaal domein, veiligheidszaken, onderwijs en burgerzaken. Aan de verwerking van deze persoonsgegevens zijn aanvullende voorwaarden gesteld, (art. 9, art. 10 AVG 'verwerking van bijzondere persoonsgegevens'). 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, bijv. in het Inkoop- en aanbestedingsbeleid.

2.4 Evaluatie

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

3. Taken en verantwoordelijkheden

3.1 Taken en rollen

Essentieel voor goed privacymanagement is een heldere verdeling van rollen, taken en verantwoordelijkheden. Hierna volgen de rollen en de daarbij behorende verantwoordlijkheden op het terrein van privacy.

3.1 a De gemeenteraad

Het college legt verantwoording af aan de gemeenteraad over de realisatie en de toepassing van de privacywetgeving en het privacybeleid. De gemeenteraad controleert het college van B&W op de uitvoering van de privacyregelgeving en het privacybeleid. De gemeenteraad wordt daartoe in staat gesteld door de verantwoordingsinformatie die het college van B&W jaarlijks verschaft.

3.1 b Het college van B&W

Het college van B&W is verantwoordelijk voor de verwerking van persoonsgegevens zoals bedoeld in de AVG. Het college van B&W stelt formeel het privacybeleid vast, delegeert de uitvoering hiervan aan de directie en legt hierover verantwoording af aan de gemeenteraad. Binnen het college van B&W valt de bescherming van persoonsgegevens onder de portefeuille van een van de portefeuillehouders. Het college van B&W stelt het beleid vast en doet de gemeenteraad voorstellen over in te zetten middelen (budget) en stelt specifieke regelingen en procedures vast. Het college van B&W legt periodiek (1 x per jaar) verantwoording af aan de gemeenteraad over het gevoerde privacybeleid.

3.1 c De directie en teammanagers

De directie en teammanagers zijn verantwoordelijk voor de inrichting van de verdere privacy-organisatie. Zij zijn naar de organisatie en medewerkers kaderstellend, sturend en monitoren de uitvoering van de privacyregelgeving en het beleid. De directie en teammanagers gezamenlijk stimuleren kennisvergaring en de bewustwording van de medewerkers. Zij voorzien in faciliteiten voor bewustwording en training. De teammanagers zijn eindverantwoordelijk voor het melden van beveiligingsincidenten en/of datalekken bij de Servicedesk, de Chief Information Security Officer (CISO) en de Functionaris voor de gegevensbescherming.

3.1 d De Chief Information Security Officer (CISO)

De CISO houdt toezicht op de informatiebeveiliging. Hij of zij ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de informatieveiligheid. De CISO bewaakt de voortgang van aanbevelingen uit audits en andere onderzoeken en adviseert over het te voeren beleid. Hij of zij is het centrale aanspreekpunt voor informatiebeveiliging en maakt, indien nodig, gebruik van het escalatiepad direct naar de directie.

3.1 e Functionaris voor de gegevensbescherming (FG)

De functionaris voor de gegevensbescherming is het aanspreekpunt voor de Autoriteit Persoonsgegevens en houdt intern toezicht op de naleving van de privacywetgeving en op het uitvoeren van het privacybeleid. In het Reglement Functionaris voor de gegevensbescherming

gemeente Súdwest-Fryslân staan de taken, bevoegdheden en verantwoordelijkheden van de functionaris voor de gegevensbescherming omschreven.

Wettelijke uitgangspunten voor de FG op grond van artikel 38 AVG zijn:

1. wordt tijdig gehoord 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 verwerkingen daarvan;
3. is onafhankelijk toezichthouder op de toepassing van de AVG en krijgt geen instructies over de uitvoering van taken;
4. treedt op als aanspreekpunt voor betrokkenen;
5. is verplicht tot geheimhouding en vertrouwelijkheid.

Taken en bevoegdheden op basis van de AVG:

- informeert, signaleert en adviseert over de verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens;
- ziet toe op de naleving van wet- en regelgeving en het beleid met betrekking tot de bescherming van persoonsgegevens ;
- werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens;
- geeft desgevraagd advies met betrekking tot de gegevensbeschermingseffect-beoordeling (PIA) en ziet toe op de uitvoering daarvan in overeenstemming met artikel 35 AVG.

3.1. f De medewerkers

Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen. Dat betekent dat iedereen zorgt draagt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.

3.2 Beveiligingsadviescommissie

Belangrijke organisatieonderdelen hebben minimaal één aanspreekpunt voor de FG. Hiervoor heeft de gemeente Súdwest-Fryslân een beveiligingsadviescommissie (BAC) ingesteld. Het overleg heeft binnen de gemeente een adviesfunctie en richt zich met name op beleid en adviseert over privacy- en informatiebeveiligingskwesties. De CISO organiseert tenminste tweemaal per jaar een overleg.

3.3 Werkgroep privacy

Vanuit het sociaal domein is in 2015 de werkgroep privacy opgericht die zich met privacy binnen het sociaal domein bezighoudt. Er wordt geschat dat 80% van alle verwerkingen van persoonsgegevens van een gemeente binnen het sociaal domein plaatsvindt. De werkgroep is inmiddels uitgebreid met vertegenwoordiging van Burgerzaken en zal in 2018 uiteindelijk een gemeentebrede werkgroep worden. Deze werkgroep organiseert de zaken die vanuit de AVG praktisch geregeld moeten worden en brengt deze tot uitvoering.

4. Maatregelen en uitgangspunten

4.1 Doelstelling

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

4.2 Maatregelen en uitgangspunten

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

4.2.1 Transparantie:

Het is van belang dat inwoners vertrouwen hebben in de zorgvuldige verwerking van hun persoonsgegevens. Inwoners krijgen inzicht in, en worden helder geïnformeerd over, hun rechten en de wijze waarop hun persoonsgegevens worden verwerkt en beheerd. Voor hen moet in ieder geval duidelijk zijn:

- welke persoonsgegevens de gemeente verzameld (wat);
- met welk doel (waarom);
- wie toegang heeft tot de gegevens (wie);
- wat de gemeente vervolgens verder doet met de gegevens (beheer);
- hoe lang de gegevens worden bewaard (bewaartermijnen);
- dat de gegevens beveiligd worden.

4.2.2 Rechtmatigheid

Gegevens worden alleen verwerkt voor zover dit wettelijk gerechtvaardigd is.

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. De functionaris voor de gegevensbescherming heeft vanaf de aanstelling in februari 2018 voorlichting en scholing verzorgd bij verschillende teams. De gehele organisatie zal meegenomen worden in de scholing en bewustwording. Er zal doorlopend aandacht worden geschonken aan de bewustwording.

4.2.4 Register van verwerkingen:

Er wordt een register opgesteld en vervolgens bijgehouden met alle verwerkingen van persoonsgegevens per proces. Deze verplichting is opgelegd door de AVG en biedt een organisatie de

mogelijkheid om ‘in control’ te zijn over de verwerkingen van persoonsgegevens. In het register worden onder andere opgenomen:

- omschrijving van de verwerking en de rechtmatigheid grondslag om deze te mogen verwerken;
- met welk doel de persoonsgegevens worden verwerkt;
- categorieën van betrokkene(n);
- categorieën persoonsgegevens;
- welke partijen er betrokken zijn bij het verwerken van de persoonsgegevens;
- welke gegevens er vastgelegd worden;
- bewaartermijnen;
- welke maatregelen Gemeente Súdwest-Fryslân heeft genomen ten aanzien van de beveiliging van de persoonsgegevens;
- welke processen en systemen er betrokken zijn bij de verwerking;
- op welke wijze de betrokkene (indien noodzakelijk) toestemming heeft gegeven voor het verwerken van de Persoonsgegevens.

4.2.5 Rechten van betrokkenen

Iedere betrokkene heeft het recht op informatie over de persoonsgegevens die de gemeente van hem of haar verwerkt, over het doel waarmee de gegevens worden verwerkt, om deze in te zien en ook in sommige gevallen om deze gegevens te verbeteren, aan te vullen of te laten verwijderen. Het college van B&W communiceert actief over deze rechten, op de gemeentelijke website en in andere uitingen. Er wordt door het college van B&W zorggedragen voor een eenvoudige en toegankelijke wijze waarop betrokkenen hun rechten kunnen uitoefenen.

4.2.6 Privacy Impact Analyses (PIA’s):

Voor (nieuwe en veranderende) processen, diensten en producten en informatiesystemen, waar persoonsgegevens worden verwerkt, worden PIA’s uitgevoerd. De AVG noemt dit een in de Nederlandse vertaling een Gegevenbeschermingseffectbeoordeling. 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 en de FG geeft na afronding een oordeel over de PIA.
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.

4.2.7 Privacy by design en Privacy by default:

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

- het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens;
- dataminimalisatie, anonimisering en pseudonimisering;

- de maatregelen die hiervoor nodig zijn.

Als vanaf de start wordt nagedacht over de privacyaspecten, dan kunnen goede oplossingen ingeregeld worden en wordt er aan de voorkant voor gezorgd dat privacy problemen zich niet kúnnen voordoen. Denk bijvoorbeeld aan logische en gerichte toegangsbeveiliging en autorisaties, encryptie van gegevens, scheiden van databestanden of het automatisch verwijderen van gegevens na een bepaalde periode of gebeurtenis. Privacy by design speelt een grote rol om in control te zijn en blijven op privacy gebied en informatiebeveiliging.

Privacy by default houdt in dat er technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat, als standaard, alléén persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel. Bijvoorbeeld door:

- een app niet de locatie te laten registeren indien dat niet nodig is;
- op de website niet standaard een vinkje bij “Ja, ik geef toestemming” in te vullen;
- als er gegevens worden gevraagd, niet meer vakken aan te bieden dan nodig zijn.

Bij het toepassen van Privacy by design en Privacy by default wordt de FG geconsulteerd.

4.2.8 Verwerkersovereenkomst:

Een verwerkersovereenkomst 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/King) als uitgangspunt genomen.

Het kan zijn dat gegevens wettelijk verplicht gedeeld dienen te worden of dat er sprake is van 2 zelfstandige samenwerkende verantwoordelijken in de zin van de privacyregelgeving. Een verwerkersovereenkomst wordt dan vervangen door een gegevensuitwisselingsovereenkomst of het opnemen van de eisen in het contract omtrent zorgvuldige omgang, beveiliging en uitwisseling, datalekken etc.

4.2.9 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. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (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 AVG bepaalt wanneer een melding moet worden gedaan bij de Autoriteit Persoonsgegevens en welke gevallen ook de betrokkenen moeten worden geïnformeerd. 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 'Protocol meldplicht datalekken gemeente Súdwest-Fryslân'.

4.2.10 Toestemming

Voor sommige gegevensverwerkingen is toestemming nodig van de betrokkenen. Dat geldt bijvoorbeeld voor sommige zaken in het sociaal domein. De AVG stelt strenge eisen aan deze toestemming. De voor verwerking verantwoordelijke moet kunnen aantonen dat de betrokkene (diegene van wie de persoonsgegevens verwerkt worden) toestemming heeft gegeven voor de verwerking van de persoonsgegeven (art. 7 AVG). Het verzoek om toestemming moet in begrijpelijke en gemakkelijke toegankelijke vorm aangeboden worden, én in duidelijke en eenvoudige taal. Daarnaast kan de betrokkene de toestemming te allen tijde intrekken.

4.2.11 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.

4.2.12 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.

Naast deze vormen van toetsing kan er ook aangesloten worden bij de standaardprocescontroles die de medewerker interne controle voor de proceseigenaren doet. Proceseigenaren kunnen zelf toetsingsvragen inzake privacy door IC laten toevoegen. Op langere termijn heeft voor interne audits inbedding in de reguliere procescontroles de voorkeur omdat privacy een rechtmatigheids- en kwaliteitsaspect is.

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