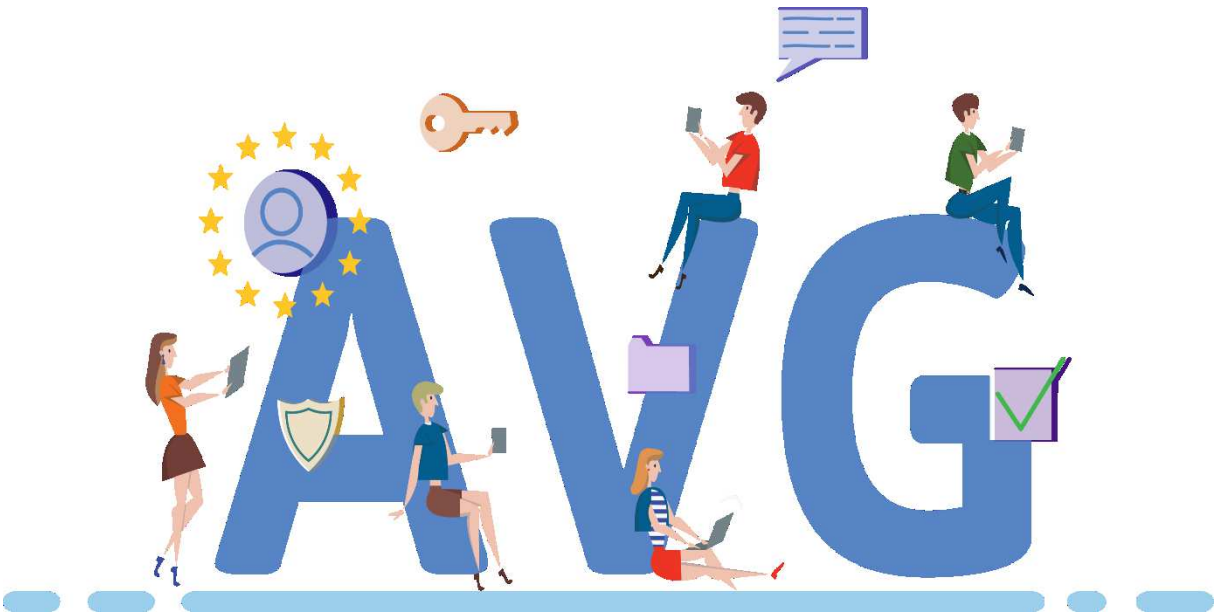
Jaarrapportage 2021 en Jaarplan 2022

gemeente Súdwest-Fryslân

Algemene verordening gegevensbescherming



Carla Aden, Functionaris gegevensbescherming

Februari 2022

Inhoudsopgave 2

Inleiding

1.1 De Algemene verordening gegevensbescherming

Op 25 mei 2022 is het 4 jaar geleden dat de Algemene verordening gegevensbescherming (Avg) van kracht werd. De Europese Unie kent hiermee één privacywet passend bij de gedigitaliseerde samenleving van nu. Iedereen die persoonsgegevens verwerkt binnen Europa, moet zich aan deze verordening houden. Het doel van de verordening is om een zorgvuldige verwerking van persoonsgegevens verplicht te stellen, om zo de privacy van de betrokkenen en hun data te waarborgen. Daarbij moeten organisaties voor betrokkenen inzichtelijk maken waarom en waarvoor persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt.
Digitalisering en de toepassing van nieuwe technologieën leiden tot veranderingen in de samenleving. Hierdoor verschuiven ook de verwachtingen die burgers hebben van de gemeentelijke dienstverlening en de omgang met de gegevens die worden toevertrouwd. De manier van omgaan met deze persoonsgegevens speelt een belangrijke rol bij het waarmaken van die verwachtingen. Om het vertrouwen van mensen en hun gevoel van veiligheid op peil te houden is daarom een goede balans nodig tussen de kansen van digitalisering en de bescherming van persoonsgegevens. De Avg voorziet in het kader om die balans te waarborgen.

Wat heeft de Avg veranderd?

De Avg heeft onder meer gezorgd voor:

- versterking en uitbreiding van privacyrechten;
- meer verantwoordelijkheden voor organisaties;
- dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

In dit document wordt het kader weergegeven, de huidige stand van zaken, met de terugblik op 2021, geschetst en daarna wordt aangegeven waaraan gewerkt gaat worden in 2022.

1.2 Verantwoordelijkheden

Het college van B&W is eindverantwoordelijk voor de verwerkingen van persoonsgegevens in de gemeente Súdwest-Fryslân. De bescherming van persoonsgegevens van betrokkenen hoort een permanent aandachtspunt te zijn van verwerkingsverantwoordelijken, bestuurders, directie, management en medewerkers. Die voortdurende aandacht zorgt ervoor dat het rekening houden met persoonsgegevens in het DNA van iedereen wordt opgenomen. Op deze manier voelt het als vanzelfsprekend de persoonsgegevens van anderen zo te behandelen zoals wij de persoonsgegevens van onszelf behandeld willen zien. Adequaat en zorgvuldig omgaan met persoonsgegevens is een blijvend proces.

Op de verwerkingen van persoonsgegevens vindt extern en intern toezicht plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dient de gemeente Súdwest-Fryslân te beschikken over een interne

toezichthouder: de Functionaris voor de Gegevensbescherming (FG). De FG ziet erop toe dat de Avg intern wordt nageleefd.
In de Avg worden de volgende taken genoemd voor de Functionaris gegevensbescherming:

- De betrokken partijen binnen een organisatie informeren en adviseren wat de verplichtingen zijn op het gebied van privacy;
- Advies verstrekken met betrekking tot de DPIA's (Data Protection Impact Assessments) en toezien op de uitvoering daarvan;
- Bewustwording bevorderen: het verzorgen van interne trainingen, opleidingen of voorlichtingsmateriaal valt hieronder;
- toezien op:
  - De naleving van de Avg en andere wetgeving op het gebied van privacy en
  - Het gevoerde beleid van de organisatie.

  De FG is geen toezichthouder met corrigerende bevoegdheden. De verwerkingsverantwoordelijke zelf is eindverantwoordelijk als er niet volgens de privacywet wordt gehandeld, de FG is niet persoonlijk verantwoordelijk of aansprakelijk.
- Samenwerken met de toezichthoudende Autoriteit (de AP in Nederland). De FG is het eerste aanspreekpunt voor de AP.

Naast de Functionaris gegevensbescherming heeft de gemeente een Privacy Officer die adviseert in privacyzaken, de verzoeken van burgers afhandelt, de bewustwording bevordert, het verwerkingsregister beheert, de DPIA's coördineert en mede uitvoert en aanspreekpunt is voor alle zaken die de bescherming van persoonsgegevens aangaat. De Functionaris gegevensbescherming en de Privacy Officer werken zeer nauw samen. Daarnaast trekken de Privacy Officer en de FG veel samen op met de CISO (Chief Information Security Officer). De Functionaris gegevensbescherming brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van de uitgevoerde werkzaamheden, bevindingen en aanbevelingen. Deze jaarrapportage 2021 en het jaarplan 2022 zijn bedoeld voor het PIT, DT, het college van B&W en de Gemeenteraad.

1.3 Maatschappelijke impact

Veel wetgeving (bv de Jeugdwet, de Wet maatschappelijke ondersteuning, de Leerplichtwet etc) schrijft het beschermen van persoonsgegevens voor. De meeste rechten van de betrokkenen (de personen van wie persoonsgegevens worden verwerkt) bestonden ook al vóór 25 mei 2018. Boetes en andere strafmaatregelen waren er ook al onder de Wet bescherming persoonsgegevens (Wbp). Alleen… de meeste organisaties deden niet veel om aan de Wbp te voldoen. Met de invoering van de Avg in 2018 waren veel organisaties bang om in een te strak kader te worden geperst. De AVG is echter niet bedoeld om geen gegevens meer uit te kunnen wisselen, maar om een ieder juist bewust te maken van hoe om te gaan met persoonsgegevens, de bescherming daarvan en biedt een kader waarbinnen dit wordt gefaciliteerd.

Met de invoering van de Algemene Verordening Gegevensbescherming is zo aan geheel Europa een sterke impuls gegeven om meer aandacht te schenken aan het onderwerp privacy en de verantwoordelijkheden die ermee samenhangen. Zeker met de toenemende digitalisering blijkt dit wettelijk kader onontbeerlijk.

1.4 Actualiteiten 2021

Afgelopen jaar geeft een aantal voorbeelden van wat er mis kan gaan bij het onvoldoende beschermen van persoonsgegevens: de Toeslagenaffaire bij de Belastingdienst[1] waarbij onrechtmatig profielen werden aangemaakt, grote datalekken zoals bijvoorbeeld bij de GGD[2] en bij Allekabels.nl[3].

Ook werd in 2021 de eerste boete opgelegd aan een gemeente: de gemeente Enschede kreeg een boete opgelegd van € 650.000 omdat er onrechtmatig (met gebruik van wifitracking) tellingen werden uitgevoerd in de binnenstad[4]. Deze tooling werd ook enige jaren gebruikt in Sneek en Bolsward en is naar aanleiding van de boete voor Enschede stopgezet in 2021.

De Autoriteit Persoonsgegevens (AP) heeft tevens het Uitvoeringsinstituut Werknemersverzekeringen (UWV) een boete van € 450.000 euro opgelegd. Het UWV had het versturen van groepsberichten niet goed beveiligd. Dat is een persoonlijke omgeving op de website van het UWV, waar werkzoekenden contact hebben met het UWV. Hierdoor waren er verschillende datalekken van persoonsgegevens, waaronder gezondheidsgegevens, van in totaal ruim 15.000 mensen. Ook de gemeente Súdwest-Fryslân beschikt over veel gezondheidsgegevens waar extra aandacht voor moet zijn. Zie ook de boete die het Amsterdamse ziekenhuis OLVG kreeg opgelegd: € 440.000 omdat het ziekenhuis tussen 2018 en 2020 te weinig maatregelen genomen had om toegang door onbevoegde medewerkers tot medische dossiers te voorkomen. Dat kwam door onvoldoende controle op wie welk dossier bekeek en ontoereikende beveiliging van de computersystemen.

Daarnaast was er diverse keren ophef over het schenden van privacy in het nieuws. Volgens een onderzoek van de Rijksuniversiteit Groningen en de NHL maken verschillende Nederlandse gemeenten gebruik van nepaccounts op sociale media[5]. Het doel van het gebruik van nepaccounts is deel te nemen aan groepen op sociale media om eventueel personen of groepen te kunnen monitoren. Of de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), die in strijd met de wet en in het geheim

---

[1] https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-discriminerende-en-onrechtmatige-werkwijze.

[2] Honderden medewerkers hadden onbevoegd toegang tot de persoons- en medische gegevens van iedereen die zich had laten testen op corona, of onderdeel uitmaakte van een bron- en contactonderzoek. Gegevens als voor- en achternamen, woonadressen, contactgegevens, burgerservicenummers (BSN), medische aandoeningen en medicatiegebruik. Deze gegevens werden opgeslagen in twee IT-systemen en via kanalen als Telegram, Snapchat en Wickr doorverkocht aan de hoogste bieder.
https://autoriteitpersoonsgegevens.nl/nl/nieuws/ggd-moet-persoonsgegevens-beter-beschermen

[3] De gegevens en wachtwoorden van meer dan 3 miljoen klanten van webshop Allekabels.nl zijn buitgemaakt bij een hack op 23 augustus 2020. Ongeveer 100.000 bankrekeningnummers (IBAN) zijn onderdeel van het lek

[4] https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-gemeente-enschede-om-wifitracking

[5]https://www.politieenwetenschap.nl/publicatie/politiekunde/2021/black-box-online-monitoring-bij-gemeenten-onderzocht-363/

gevoelige gegevens over burgers verzamelde en verspreidde. Medewerkers van de NCTV gebruikten nepaccounts op sociale media om politici, religieuze voormannen en activisten te volgen. Ook spoorde de NCTV gemeenten aan om private bedrijven in te zetten voor onderzoek in gebedshuizen. De Autoriteit persoonsgegevens wil mede naar aanleiding van deze zaken een verbod instellen op het online volgen van personen.

1.5 Waarborgen voor burgers

Voor burgers heeft de Algemene Verordening Gegevensbescherming direct effect. Als persoon heb je sterke rechten om controle uit te oefenen over je eigen persoonsgegevens. De mogelijkheid om je recht te halen is meer op de voorgrond komen te staan. Als het goed is, licht elke organisatie toe hoe persoonsgegevens worden verwerkt, wie verantwoordelijk is voor de verwerking, hoe lang gegevens worden bewaard, en met wie (en waarom) de persoonsgegevens worden gedeeld. Dit zijn allemaal zaken die de Algemene Verordening Gegevensbescherming regelt. Privacy is een grondrecht. En een voorwaarde om vrij te zijn in wie je bent en wat je doet. Privacy gaat erover dat mensen regie houden over hun gegevens. Het gaat erom dat we niet continu gevolgd worden, dat onze medische gegevens veilig zijn, dat we iets kunnen doen tegen een automatisch genomen besluit over ons. Het gaat over zeggenschap over onze eigen persoonsgegevens. In een vrije, democratische samenleving moeten mensen erop kunnen vertrouwen dat zorgvuldig om wordt gegaan met hun gegevens.

Voor organisaties betekent de Avg dat aantoonbaar moet worden voldaan aan de regelgeving en dat daarvan rekenschap dient te worden afgelegd aan de burger.

1.6 Autoriteit Persoonsgegevens

De Nederlandse toezichthouder, de Autoriteit Persoonsgegevens, heeft aangegeven voor de jaren 2020-2023 3 focusgebieden (bijlage 1, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/infographic_focus_ap_2020-2023.pdf) te onderkennen:

Focusgebied 2 raakt gemeenten direct en vraagt scherpe aandacht voor de manier van

werken bij de gemeenten. De Avg vereist dat de gemeente Súdwest-Fryslân *zorgvuldig en rechtmatig* met persoonsgegevens omgaat en *aantoonbaar* aan de Avg voldoet.

Voldoen aan de Avg is niet iets eenmaligs door bijvoorbeeld een implementatietraject af te vinken. Privacy en de bescherming van persoonsgegevens vereist continue aandacht, bewustwording bij en voor medewerkers, monitoring en het inzetten van verbeteringen. Door de bescherming van persoonsgegevens serieus te nemen wordt:

- gewerkt aan het inregelen van de huidige noodzakelijke maatregelen op het terrein van informatiebeveiliging en privacy die zo belangrijk zijn door toenemende digitalisering en de dreigingen die hiermee gepaard gaan;
- invulling gegeven aan het begrip betrouwbare overheid en
- kwalitatief goede en zorgvuldige dienstverlening georganiseerd.

1.7 Wettelijke eisen Avg

Hieronder volgen de belangrijkste wettelijke eisen uit de Avg met daaraan gekoppeld een praktische vertaling naar onze gemeentelijke dagelijkse praktijk:

- Transparantie: de persoon van wie de gegevens verwerkt worden, is hiervan op de hoogte, heeft hiervoor toestemming gegeven en kent zijn rechten (art. 5 lid 1a AVG).

  Praktijk: Vertaald naar onze organisatie betekent dit dat de burger precies weet wat we met zijn/haar gegevens doen, waar deze worden opgeslagen, hoe lang we de gegevens bewaren en wie toegang heeft tot de gegevens.

- Doelbeperking: de persoonsgegevens worden voor een welbepaald gewettigd doel verzameld, en mogen niet voor andere zaken gebruikt worden (art. 5 lid 1b AVG).

  Praktijk: De gegevens mogen alleen worden gebruikt voor het doel waarvoor ze zijn uitgevraagd. Dus de gegevens die op basis van bv de Wet maatschappelijke ondersteuning (Wmo) zijn gevraagd mogen absoluut niet voor een ander doel gebruikt worden.

- Gegevensbeperking, dataminimalisatie: enkel de gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld of opgeslagen (art. 5 lid 1c AVG).

  Praktijk: Alleen de gegevens die nodig zijn om de gevraagde dienstverlening te kunnen geven mogen uitgevraagd of opgeslagen worden. Streven moet zijn om zo weinig mogelijk data te gebruiken. Dat maakt de burger én de organisatie minder kwetsbaar.

- Juistheid: de persoonsgegevens moeten correct zijn en blijven (art. 5 lid 1d AVG).

  Praktijk: Dit vraagt zeer zorgvuldig te zijn met de gegevens: maak geen kopieën, deel geen gegevens en/of koppelingen zonder wettelijke grondslag.

- Bewaarbeperking: de persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel (art. 5 lid 1e AVG).

  Praktijk: Vraagt om discipline om op te ruimen. Als de gegevens niet meer nodig zijn voor de gevraagde dienstverlening dan dienen deze vernietigd te worden. Langer bewaren van gegevens dan noodzakelijk is onrechtmatig en veroorzaakt een datalek. De neiging om zoveel mogelijk te bewaren omdat dat 'handig' is, is hiermee verleden tijd.

- Integriteit en vertrouwelijkheid: de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging (art. 5 lid 1f AVG).

  Praktijk: Iedere applicatie of systeem kent een aantal gebruikers die op basis van hun taken en werkzaamheden toegang hebben. Iemand mag alleen toegang hebben tot die gegevens die noodzakelijk zijn om haar/zijn taken uit te kunnen voeren. Deze eis vraagt om goede autorisaties en het controleren van de toegang tot gegevens. In de managementletter wordt voor dit onderdeel prioriteit gevraagd.

- Verantwoording: de verantwoordelijke moet kunnen aantonen aan deze regels te voldoen (art. 5 lid 2 AVG).

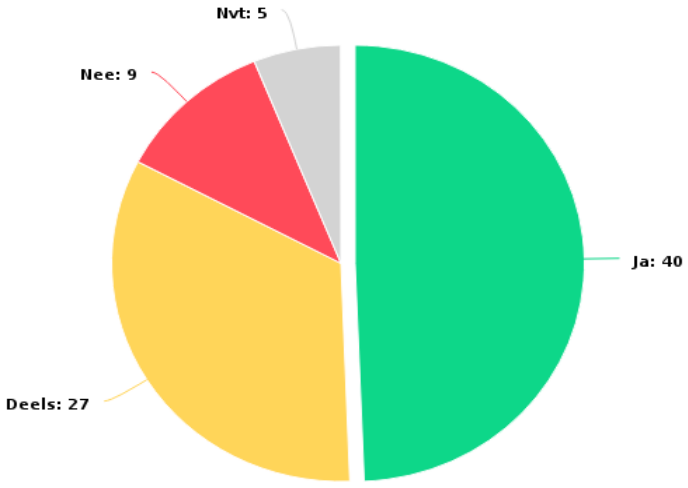
  Praktijk: Dit vertaalt zich in een administratieve organisatie rondom de persoonsgegevens: een verwerkingsregister, rapportages, procedures, procesafspraken, controles, openbaarmaking werkwijzen, afleggen van verantwoording door verantwoordelijken.

Terugkijken 2021

2.1 Overzicht: meting en rapportage 2021 aan de hand van het normenkader

VNG Realisatie heeft criteria ontwikkeld om de Avg te vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. Hiermee beoogt de VNG gemeenten concrete handvatten te bieden om een goede omgang met persoonsgegevens in de gehele organisatie te waarborgen.
Het onderwerp 'privacy' is in de rapportagetool opgesplitst in 9 onderdelen, welke gezamenlijk alle aspecten van gegevensbescherming dekken. De 9 onderdelen zijn: Privacybeleid, Privacymanagement, Personeel en organisatie, Privacyservices, Verwerkersovereenkomsten, Verwerkingsregister, Privacycompliance, DPIA's en Informatiebeveiliging. Er is geen volgorde: de criteria dienen in onderlinge samenhang te worden gelezen. De criteria verwijzen ook naar relevante criteria uit een ander onderdeel: het ene criterium kan niet geborgd worden als het andere criterium van het andere onderwerp niet waargemaakt is. Alle criteria tezamen beschrijven de 'geborgde situatie' voor een gemiddelde gemeente per onderwerp.
Dit borgingsproduct is een 'levend' document: het kan ieder gewenst moment opnieuw doorgelopen worden en zal 1 keer per jaar worden voorgelegd aan het bestuur. Op deze manier blijft het document actueel en wordt er verantwoording afgelegd conform artikel 38 Avg.

Hieronder wordt eerst de stand van zaken **over 2021** weergegeven:

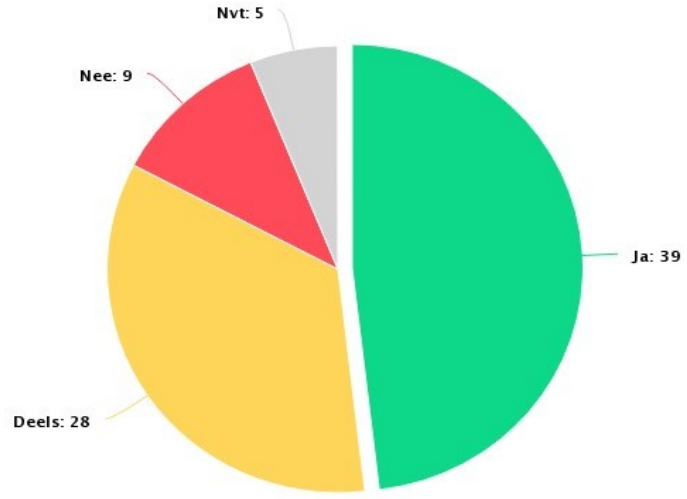


In januari 2022 voldoet de gemeente geheel aan 40 normen, gedeeltelijk aan 27 normen en aan 9 normen wordt nog niet voldaan.

Hoofdstukken 2021	Aantal normen	% Score
1 Privacybeleid	4	63%
2 Privacymanagement	27	70%
3 Personeel en privacy	8	58%
4 Privacy services	14	89%
5 Verwerkersovereenkomsten	4	63%
6 Verwerkingsregister	4	83%
7 Privacy compliance op verwerkingsniveau	6	17%
8 DPIA's op verwerkingsniveau	6	83%
9 Informatiebeveiliging	8	81%
Totaal	**81**	**70%**

Meting over het jaar 2020

Hieronder de resultaten van de meting over het jaar **2020**:



In december 2020 (een dik jaar geleden) voldeed de gemeente geheel aan 39 normen, gedeeltelijk aan 28 normen en aan 9 normen werd nog niet voldaan.

Hoofdstukken (2020)	Aantal normen	% Score
1 Privacybeleid	4	50%
2 Privacymanagement	27	64%
3 Personeel en privacy	8	43%
4 Privacy services	14	82%
5 Verwerkersovereenkomsten	4	50%
6 Verwerkingsregister	4	33%
7 Privacy compliance op verwerkingsniveau	6	8%
8 DPIA's op verwerkingsniveau	6	40%
9 Informatiebeveiliging	8	81%
Totaal	**81**	**59%**

2.2 Conclusie over de voortgang in 2021

Gezien de metingen is er in 2021 een mooie stabiele situatie ontstaan én vooruitgang geboekt. De overall-score is van 59% naar 70% gegaan.
Uitgelicht:

- de bewustwording onder managers en medewerkers is gegroeid,
- het verwerkingsregister is geheel doorgenomen en up-to-date gebracht,
- de DPIA-werkgroep draait zeer goed en
- er is meer gewerkt aan goede afspraken met derden in verwerkersovereenkomsten.

Onderwerpen waar nog meer aandacht aan besteed kan worden:

- bewustwording op alle niveaus,
- compliance op verwerkingsniveau,
- en beleid.

In het jaarplan voor 2022 zullen deze onderwerpen opgenomen worden.

De belangrijkste constateringen over 2021 zijn:

1. Bewustwording bij de medewerkers blijkt opnieuw de zeer belangrijke pijler in de bescherming van gegevens. In 2021 is het ondanks het vele thuiswerken toch gelukt op afstand invulling te geven aan dit gegeven. Intranet is regelmatig benut om te communiceren over het thema. Tevens heeft het eerste half jaar een bewustwordingscampagne gedraaid: Sir Askalot. Iedere week kregen alle medewerkers een meerkeuzevraag over Informatiebeveiliging en/of privacy om op een laagdrempelige manier meer over deze onderwerpen te kunnen leren.
2. Het uitvoeren van Data Protection Impact Assessments (DPIA’s) loopt zeer goed. Zie aparte toelichting onder kopje DPIA’s op bladzijde 13.
3. Er worden regelmatig datalekken gemeld. Dat is realistisch en duidt op een veilige werkomgeving. In de volgende paragraaf wordt iets dieper op dit onderwerp ingegaan.

4. Uitwisselingen en overdragen van persoonsgegevens intern en met derden moeten altijd op een wettelijke grondslag zijn gebaseerd. Als die er niet is dienen de partijen zeer duidelijke en openbare afspraken te maken. In 2021 is hiermee begonnen, maar in 2022 behoeft dit onderdeel verdere aandacht en uitwerking.
5. In het jaar 2021 zijn veel wisselingen geweest in het management. Dat is van invloed op het gezamenlijke bewustzijn op het gebied van de privacyregels: verantwoordelijkheden zijn veranderd of zijn wellicht nog niet bekend. Dit beïnvloedt de governance en het besef van verantwoordelijkheden.
6. Het verwerkingsregister was bij de invoering van de Avg in 2018 opgesteld en is in 2020 en 2021 geheel doorgenomen en aangepast. Het register vormt een belangrijke basis voor het in-control zijn voor het onderwerp privacy.
7. In 2021 bleek dat er in het kader van de Wet Politiegegevens (Wpg) audits uitgevoerd te moeten worden. De Privacy Officer heeft dit opgepakt en er samen met 2 medewerkers uit de teams voor gezorgd dat voldaan werd aan de verplichtingen op basis van de Wpg. Dit onderwerp dient in 2022 structureel in de organisatie belegd te worden.
8. Beleidsstukken in het kader van privacy bieden naast het wettelijke kader de basis voor de gemeente om op te acteren. In 2021 zijn nog niet alle benodigde stukken gereed gekomen. Voor 2022 staan daarom de volgende beleidsstukken op de agenda: Privacy in het sociaal domein, Algemeen privacybeleid en Beleid inzake het verwerken van persoonsgegevens op basis van de Wet Politiegegevens (Wpg).

2.3 Datalekken

Door de Wet meldplicht datalekken en de Avg zijn organisaties verplicht (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een (ernstig) datalek hebben. En soms moeten het datalek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

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. Of zonder dat dit wettelijk is toegestaan. In 2021 heeft de gemeente Súdwest-Fryslân 26 datalekken (in 2020 waren dat er 8) gehad die bij de Functionaris gegevensbescherming zijn gemeld en daarvan zijn er vervolgens 8 gemeld bij de Autoriteit Persoonsgegevens. In 10 gevallen is (zijn) de betrokkene(n) geïnformeerd over het datalek. De oorzaken van de datalekken zijn zeer divers. Voorbeelden:

- Er wordt per abuis een mail of post met persoonsgegevens naar een verkeerde geadresseerde gestuurd (dit is de meest voorkomende oorzaak van de datalekken in onze gemeente in 2021)
- Er zijn gegevens (telefoon, dossiers) kwijtgeraakt
- Intern onbevoegde toegang tot persoonsgegevens
- Cybercrime gerelateerde gebeurtenissen

Onder medewerkers is steeds meer duidelijk wanneer er sprake is van een mogelijk datalek. De meldingen kloppen bijna altijd en er wordt snel ondersteuning of advies gevraagd. Hierdoor is het mogelijk om te voldoen aan de wettelijke verplichtingen van tijdig melden bij

de Autoriteit Persoonsgegevens en/of betrokkenen en kunnen er, waar nodig, maatregelen getroffen worden.

2.4 Rechten van betrokkenen

Mensen hebben verschillende rechten om controle te houden over hun persoonsgegevens:

- Recht op inzage. Dat is het recht van mensen om onder meer een kopie te ontvangen van de persoonsgegevens die worden verwerkt.
- Recht op vergetelheid. Mensen hebben het recht om 'vergeten' te worden.
- Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die worden verwerkt te laten wijzigen.
- Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten en het absolute verbod op geautomatiseerde besluiten.
- Het recht om bezwaar te maken tegen de gegevensverwerking.
- Ten slotte hebben mensen recht op duidelijke informatie over wat er met hun persoonsgegevens gebeurd. Onder de AVG moet iedere organisatie aan een aantal specifieke eisen voldoen. De website van de gemeente geeft uitgebreid informatie over de rechten van betrokkenen.

Op laagdrempelige wijze heeft de gemeente het mogelijk gemaakt dat de burger zijn/haar rechten kan verzilveren. In 2021 zijn de volgende verzoeken afgehandeld:

- Verzoek tot recht op inzage: 8
- Verzoek tot verwijdering: 2
- Verzoek tot rectificatie: 1

De afhandeling heeft steeds binnen daarvoor geldende termijn plaatsgevonden.

Klachten bij de gemeente
Er zijn 4 klachten ingediend over de uitvoering en toepassing van de Avg door de gemeente Súdwest-Fryslân. Deze zijn door de klachtenfunctionaris afgehandeld.

Klacht bij de Autoriteit Persoonsgegevens
In 2021 is er (voor zover bekend) over de gemeente één klacht ingediend bij de Autoriteit Persoonsgegevens. De klacht is ongegrond verklaard waarna de betrokkene in bezwaar is gegaan. Ook het bezwaarschrift is door de Autoriteit Persoonsgegevens ongegrond verklaard. Betrokkene heeft vervolgens beroep ingesteld bij de Rechtbank. De zitting heeft in december 2021 plaatsgevonden, maar er is in 2021 nog geen uitspraak gedaan.

2.5 DPIA's

Onder de Algemene verordening gegevensbescherming zijn organisaties verplicht Data Protection Impact Assessments (DPIA's) uit te voeren. Dit is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Vervolgens kunnen

daarna maatregelen worden ingesteld om de risico's te verkleinen. DPIA's zijn verplicht bij risicovolle verwerkingen en gewenst bij alle verwerkingen.

In 2020 is er een interne werkgroep gestart met het maken van DPIA's. De werkgroep bestaat uit een senior juridisch adviseur, een inkoopadviseur, de beleidsadviseur planning & control en de privacy officer. De werkgroep-leden hebben een uitgebreide opleiding voor het uitvoeren van DPIA's gevolgd en voeren deze sinds 2020 regelmatig uit. De onderwerpen waarvoor in 2021 een DPIA op is uitgevoerd zijn:

- Druppelsysteem: de 'druppel' wordt door alle medewerkers gebruikt voor toegang en beveiliging van gebouwen en enkele apparaten
- Camera-inzet: gebruik van camera's bij gemeentelijke gebouwen en voorzieningen
- TRS: nieuw toezichtregistratie systeem van de BOA's (Bijzondere Opsporings-Ambtenaren)
- Wet gemeentelijke schuldhulpverlening: wijziging met gevolgen voor het proces en werkwijze
- Wifi tracking in de binnenstad: inzet wifitracking om publieksstromen te meten in de binnenstad van Sneek en Bolsward

Van start gegaan in 2021 en bijna afgerond:

- Centric leefomgeving
- Wet inburgering

3. Jaarplan 2022

De meting over 2021 geeft duidelijk weer welke normen nog geïmplementeerd dienen te worden of waar verder versterkt kan worden. Voor het jaar 2022 is gekozen voor in ieder geval de volgende acties:

1. **Beleid:**

- Algemeen privacy-beleid
- Beleid privacy in het sociaal domein
- Beleid Wet Politiegegevens en de verwerking van persoonsgegevens

2. **Privacymanagement**

- Teamleiders zijn (eind-) verantwoordelijk voor de verwerkingen van persoonsgegevens binnen hun team. Regelmatig bezoekt de privacy officer de teamleiders voor periodiek overleg (privacy aangelegenheden, het verwerkingsregister, eventuele nieuwe verwerkingen en DPIA's).
- Het jaarplan met de meting is een cyclisch PDCA-beheersingsproces. Borging vindt plaats door twee maal per jaar de voortgang te bespreken met het DT en met de portefeuillehouder privacy in februari en augustus. Metingen in december/januari en juli. Voordat de voortgang met de portefeuillehouder privacy besproken wordt, wordt de voortgang aan het PIT en het DT voorgelegd.

3. **Personeel en privacy**

- Gezamenlijk optrekken in het kader van bewustwording met de CISO die gaat over de Informatiebeveiliging.
- Via Intranet en andere kanalen worden medewerkers maandelijks geïnformeerd over privacy-onderwerpen en informatiebeveiliging.
- Voorlichting verzorgen voor nieuwe medewerkers. Actief zijn bij het on-boarden.

4. **Privacy services**

- Periodiek (2x per jaar) het PIT, DT en de portefeuillehouder privacy informeren over ingediende inzageverzoeken en het datalekken.

5. **Overeenkomsten met derden (gezamenlijke verantwoordelijken) en verwerkers**

- Alle samenwerkingsverbanden worden in kaart gebracht en dienen te voldoen aan de Avg.
- Betrokkenheid EPA-pilot (samenwerking in aanpak voor de doelgroep met Ernstig Psychiatrische Aandoeningen)
- Bijhouden al bestaande overeenkomsten.

6. Verwerkingsregister

- Bijhouden. Geen extra acties nodig.

7. Privacy compliance op verwerkingsniveau

- Wpg-taken beleggen.
- Evaluatie Wmo processen BG en HH op het gebied van privacy.
- Project inkomstenverrekening Participatiewet.
- Nu de basis op orde is een plan maken om dit onderdeel verder op te pakken.

8. DPIA's

- Proceseigenaren indien nodig informeren over hun verantwoordelijkheden m.b.t. DPIA's.
- Voortzetting uitvoeren van DPIA’s.

9. Informatiebeveiliging

- Samenwerking met CISO continueren.
- Gezamenlijk met JVZ, CISO en FG een Cybersecurity-crisisplan opstellen.

Bijlage: Infographic focus AP 2020-2023

Veel van het gemak in ons leven komt door technologie en digitalisering. We hebben allemaal een smart phone in onze broekzak en steeds meer mensen maken gebruik van een slimme meter, hebben slimme speakers en apparaten met stemherkenning. Ook onze diensten regelen we steeds meer online; van onze bankzaken tot de aangifte van onze belasting tot het vinden van een partner.

Al deze apparaten en diensten verzamelen persoonlijke gegevens waardoor ze steeds meer van ons weten. Niets voor niets wordt inmiddels gezegd dat zoekmachines en sociale media op basis van onze zoekgegevens en berichten ons beter kennen dan onze naasten. Uit de grote hoeveelheid data kun je immers afleiden wat onze seksuele voorkeur is, op welke partij we stemmen, hoe vaak we onze huisarts of specialist hebben bezocht en waar we ons geld aan uitgeven. Anders gezegd, er wordt steeds meer over ons vastgelegd, ons leven wordt steeds beter gedocumenteerd zonder dat we precies weten wat er met die gegevens gebeurt en wie er toegang toe heeft. Dit maakt ons en onze democratische rechtstaat kwetsbaar.

In deze digitale samenleving is de bescherming van persoonsgegevens (dataprotectie) essentieel. Daarom is het recht op gegevensbescherming opgenomen in het Handvest van de grondrechten van de Europese Unie. Het is een belangrijk grondrecht dat er is er om ons tegen misbruik te beschermen. Het gaat in de kern over zeggenschap, over autonomie, over dat wij als burgers zelf gaan over wat we met wie delen. Kortom, het fundamentele recht op bescherming van privacy moet voorkomen dat de fundamenten van onze rechtsorde, vrije wil en onze autonomie eroderen.

De Autoriteit Persoonsgegevens (AP) heeft hierin een belangrijke taak. De AP is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. Wij zijn onderdeel van een Europees samenwerkingsverband van toezichthouders. Ons toezichtveld is omvangrijk: nationale en internationale bedrijven en organisaties, de gehele overheid – inclusief politie en justitie – en ook verenigingen, scholen, stichtingen en individuele burgers. Dit doen we niet alleen in Nederland; data kennen immers geen grenzen. Het toezicht van de AP is daarom bij uitstek grensoverschrijdend. Samen met onze Europese collega toezichthouders geven we voorlichting, doen we onderzoek en delen we boetes uit aan bedrijven en organisaties die zich niet aan de wet houden. Daarbij willen we innovatie de ruimte geven, om gemak en welvaart te stimuleren. Het is onze overtuiging dat innovatie hand in hand kan en moet gaan met de bescherming van persoonsgegevens. Bij nieuwe technologieën bevordert de AP daarom privacy by design en privacy by default.

De 'Focus Autoriteit Persoonsgegevens 2020-2023' beschrijft welke ontwikkelingen en risico's wij zien en waar wij de komende periode onze aandacht aan besteden om de bescherming van persoonsgegevens te borgen.

Katja Mur, Monique Verdier en Aleid Wolfsen
Bestuur Autoriteit Persoonsgegevens

AUTORITEIT
PERSOONSGEGEVENS