Jaarrapportage 2022 en Jaarplan 2023

Algemene verordening gegevensbescherming

Carla Aden, Functionaris gegevensbescherming

Januari 2023

Inhoudsopgave

WOORD VOORAF

Voor u ligt de jaarrapportage 2022 en het Jaarplan voor 2023 inzake de Algemene verordening gegevensbescherming (Avg) van de gemeente Súdwest-Fryslân. Met deze jaarlijkse rapportage wordt u geïnformeerd over de stand van zeken met betrekking tot de bescherming van persoonsgegevens binnen de gemeente zoals voorgeschreven in de Algemene verordening gegevensbescherming. Tevens wordt in het jaarplan 2023 aangegeven welke acties uitgevoerd zullen worden het komende jaar.

Sneek, januari 2023
Carla Aden, Functionaris gegevensbescherming

Inleiding

1.1 De Algemene verordening gegevensbescherming

Op 25 mei 2023 is het alweer 5 jaar geleden dat de Algemene verordening gegevensbescherming (Avg) van kracht werd. De Europese Unie kent met deze verordening één privacywet geldend voor alle EU-lidstaten 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 van betrokkenen;
- meer verantwoordelijkheden voor organisaties;
- dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen. Een eenduidig kader voor heel Europa en haar inwoners.

Voor de gemeente betekenen bovenstaande punten o.a. dat inwoners vragen kunnen stellen over hoe er met hun persoonsgegevens wordt omgegaan, dat de gemeente transparant moet zijn en verantwoording af moet leggen over hoe zij met persoonsgegevens omgaan en dat bij schending van deze privacyrechten er consequenties zijn.

In dit document wordt het kader weergegeven, de huidige stand van zaken, met de terugblik op 2022, geschetst en daarna wordt aangegeven waaraan gewerkt gaat worden in 2023.

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. De AVG vereist dat de FG autonoom kan handelen bij de uitoefening van zijn taken. De FG dient tijdig te worden betrokken en geïnformeerd, krijgt geen instructies met betrekking tot de uitvoering van zijn taken, beschikt over voldoende middelen en heeft een volledig onafhankelijke positie.
In de artikel 39 van de Avg worden de volgende taken belegd bij 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) en de ISO (Information security officer: sinds september 2022 in dienst) en met de Integriteits-coördinator. De Functionaris gegevensbescherming brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van de uitgevoerde werkzaamheden, bevindingen en aanbevelingen. Deze jaarrapportage 2022 en het jaarplan 2023 zijn bedoeld voor Directieteam, het college van B&W en de Gemeenteraad.

1.3 Actualiteiten 2022

De Belastingdienst heeft opnieuw in 2022 een aanvullende AVG-boete gekregen vanwege zijn handelen in het toeslagenschandaal. De Autoriteit Persoonsgegevens legt een recordboete van 3,7 miljoen euro op vanwege het beruchte Fraude Signalering Voorziening-systeem.

Het ministerie van Buitenlandse Zaken kreeg ongemeen harde kritiek van de Autoriteit Persoonsgegevens (AP). Bij het verlenen van visa heeft het departement jarenlang, op grote schaal en op ernstige wijze de wet overtreden. Dat levert een forse boete op van tot nu toe € 565.000. AP vindt dat Buitenlandse Zaken ernstig nalatig is geweest en dat nog steeds is. De beveiliging van het 'Nationaal Visum Informatie Systeem' is onvoldoende, met bijvoorbeeld als risico dat onbevoegden dossiers kunnen inzien en wijzigen. Daarnaast werden visumaanvragers ontoereikend geïnformeerd over het delen van hun gegevens met andere partijen.

De Gelderse gemeenten Buren en Neder-Betuwe zijn getroffen door een aanval met ransomware. Criminelen hebben honderdduizenden bestanden buitgemaakt en te koop aangeboden op het dark web, het niet direct vindbare deel van internet. De ransomware-aanval vond op 1 april plaats, meldt de gemeente Buren. Er is zo'n 130 gigabyte aan gegevens gestolen. Dat zijn ruim 730.000 bestanden. Deze bestanden bestaan onder andere uit paspoortgegevens, BSN's, personeelsdossiers enzovoort. De gemeenten zijn nog steeds bezig met herstelwerkzaamheden.

De Politie kreeg een boete wegens privacyschendingen bij inzet camera-auto's Rotterdam. De Autoriteit Persoonsgegevens heeft de Nederlandse politie een boete van € 50.000 opgelegd. In Rotterdam zijn tijdens een periode in 2020 in de coronatijd camera-auto's ingezet, maar daarvan waren de privacyrisico's niet in kaart gebracht en er zijn te veel beelden verzameld. Volgens de Autoriteit Persoonsgegevens heeft de politie met de specifieke inzet van de camera-auto's de wet op meerdere manieren overtreden.

Bij de gemeente Súdwest-Fryslân zijn tot op heden geen schendingen geconstateerd of in onderzoek genomen door de AP.

1.4 Maatschappelijke impact

Veel wetgeving (bv de Jeugdwet, de Wet maatschappelijke ondersteuning, de Leerplichtwet etc.) schrijft het beschermen van persoonsgegevens voor. 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.

De Algemene Verordening Gegevensbescherming heeft 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, de daarbij horende verantwoordelijkheden en de cyberdreigingen blijkt dit wettelijk kader onontbeerlijk.

In de vorige paragraaf zijn een aantal voorbeelden genoemd van wat er verkeerd kan gaan en hoe de kansen door digitalisering tegelijkertijd nieuwe risico's voor de beveiliging en bescherming van gegevens oplevert. Door die risico's in kaart te brengen en er gepaste maatregelen op toe te passen kunnen incidenten en inbreuken voorkomen worden. Er zijn in

2022 diverse documenten opgeleverd die ondersteuning bieden hierin. Twee daarvan worden hier benoemd:

1. De ALV van de VNG (Vereniging Nederlandse gemeentes) heeft in dit kader unaniem voor **de *Principes voor de Digitale Samenleving*** https://vng.nl/sites/default/files/2022-12/Principes-voor-de-Digitale-Samenleving.pdf gestemd. Deze principes geven weer hoe gemeenten omgaan met digitalisering en innovatieve technologie in de openbaar toegankelijke ruimte. De principes bieden gemeenten ambities en een gezamenlijk kader voor het omgaan met dilemma's die digitalisering met zich meebrengt. Bijvoorbeeld bij het verzamelen en gebruiken van data voor beleid. Publieke waarden, zoals democratische besluitvorming, maatschappelijke waarden en transparantie staan daarbij centraal. *"Het uitgangspunt is dat mensen zich anoniem en onbespied in de openbare ruimte moeten kunnen bewegen. Wij zien dat sensor- en cameratechnologie (en de achterliggende data- en algoritme-infrastructuur) dagelijks krachtiger, makkelijker toepasbaar en goedkoper wordt. En daarmee breed inzetbaar voor maatschappelijk nut. Maar die inzet moet steeds vooraf gegaan worden door een afweging tussen betrokken waarden, voor afzonderlijke toepassingen en systemen in samenhang. Het risico bestaat immers dat door introduceren en verbinden van technologie onbewust, 'per ongeluk', een surveillance-infrastructuur wordt aangelegd. Specifiek voor de inzet van biometrische surveillancetechnologie, zoals gezichtsherkenning, en het individueel volgen van mensen maken wij de afweging dat hun nut niet in verhouding staat tot de risico's voor publieke waarden. Gemeenten sluiten deze technologie voor hun taakuitoefening daarom uit. Voor hun positie als ketenpartner met de politie gelden maximale waarborgen, zoals een heldere juridische basis*."(bladzijde 6)

2. De Informatiebeveiligingsdienst (IBD) van de VNG heeft het **Dreigingsbeeld 2023-2024** opgesteld:
   https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/
   De IBD wil met deze publicatie gemeenten ondersteunen bij het in beeld krijgen en managen van de risico's voor inwoners, ondernemers, de ambtelijke organisatie, de politiek en het bestuur. De dreigingen kunnen gepareerd worden door regie te voeren op integraal risicomanagement. En door uit te dragen dat informatieveiligheid en het beschermen van gegevens niet iets is van de ICT-afdeling, maar van alle mensen in de hele organisatie. Deze publicatie schetst de belangrijkste dreigingen en de zaken die binnen gemeenten een rol spelen. De IBD sluit dit dreigingsbeeld af met een stapsgewijs handelingsperspectief en het benoemen van 6 succesfactoren.

   De 6 succesfactoren:
1. *Financiën*: reserveer een vast percentage in het budget voor informatiebeveiliging en privacy (bescherming persoonsgegevens)
2. *Techniek*: de basismaatregelen tegen ransomware zijn op orde
3. *Eigenaarschap management:* Informatiebeveiliging en gegevensbescherming staan op de managementagenda

4. *Organisatie:* positionering Chief Information Officer (CISO), Functionaris gegevensbescherming (FG), Privacy Officer (PO) van belang naast een veilige cultuur
5. *Samenwerkingsverbanden:* maak afspraken en zie erop toe
6. *De factor mens:* investeren in bewustwording

Door opvolging te geven aan deze succesfactoren in de gemeente Súdwest-Fryslân kan de veiligheid en bescherming van persoonsgegevens op een hoger niveau worden gebracht. In het jaarplan 2023 komen een viertal van deze succesfactoren terug.

1.5 Ontwikkelingen

Wet politie gegevens (Wpg)

Wanneer een gemeente haar taken uitvoert en daarbij persoonsgegevens verwerkt, is de Algemene Verordening Gegevensbescherming (Avg) altijd van toepassing. Maar als een Buitengewoon opsporingsambtenaar (boa) persoonsgegevens verwerkt, dan ligt dat soms net even anders. Die gegevens kunnen namelijk onder verschillende wettelijke regimes vallen. Persoonsgegevens die een boa verwerkt in zijn rol als toezichthouder, vallen onder de Avg. De gegevens die de boa echter als opsporingsambtenaar verwerkt, vallen onder de Wet politiegegevens (Wpg). Voor gegevens die onder de Wpg worden verwerkt (voor opsporing dus), gelden andere regels dan onder de Avg. Bijvoorbeeld andere bewaartermijnen, of andere eisen die gelden bij het onderling delen van gegevens. Het is daarom van belang dat de gegevensverwerkingen die onder de Wpg vallen, andere kenmerken en aandacht krijgen dan de gegevensverwerkingen die onder de Avg vallen. Om vast te kunnen stellen dat gemeenten dit bij hun verwerkingen conform de wettelijke eisen hebben toegepast, wordt onder andere de audit Wet politiegegevens uitgevoerd. De Wpg is per 1-1-2019 ingrijpend gewijzigd waardoor er een aantal nieuwe verplichtingen voor boa-werkgevers zijn gaan gelden. In 2021 en 2022 is in bij de gemeente Súdwest-Fryslân een start gemaakt om te voldoen aan de wettelijke verplichtingen, maar aan het einde van 2022 zijn nog niet alle wettelijke verplichtingen voldoende en duidelijk belegd.

Algoritme-register

De privacywaakhond Autoriteit Persoonsgegevens (AP) beoordeelt voortaan ook algoritmes bij organisaties en bedrijven. Het nieuwe toezicht moet onder meer discriminatie door computers aanpakken. Een algoritme is kort gezegd een verzameling regels die een computer volgt om tot een doel te komen. Het kan mensen raken als algoritmes met verkeerde informatie getraind zijn. Er kan dan bijvoorbeeld vooringenomenheid en discriminatie in sluipen (zoals bij de Belastingdienst is gebeurd in de Toeslagenaffaire).
Het moet veel transparanter worden hoe algoritmes precies werken. Burgers moeten meer controle kunnen krijgen over hoe hun gegevens door algoritmes gebruikt mogen worden. Volgens het kabinet en de AP moet digitale technologie de mens dienen in plaats van andersom. Daarom moeten bedrijven eerst een risicoanalyse maken, voordat ze algoritmes inzetten om bijvoorbeeld werkzaamheden van mensen te automatiseren.

Op 5 april 2022 heeft de Tweede Kamer hierover een motie aangenomen waarbij werd opgeroepen een Impact Assessment Mensenrechten en Algoritmes ('IAMA') verplicht in te zetten voordat algoritmes worden toegepast bij het evalueren van en nemen van beslissingen over mensen. Overheden zullen - in ieder geval hoog risico - algoritmes moeten publiceren in een (decentraal) algoritmeregister. Dit onderwerp dient in 2023 binnen de gemeente opgepakt te worden.

1.6 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.

1.7 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.

1.8 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.

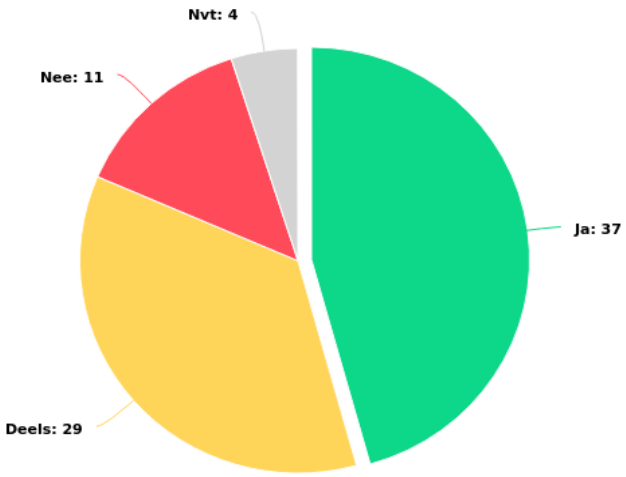
Terugkijken 2022

2.1 Overzicht: meting en rapportage 2022 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.

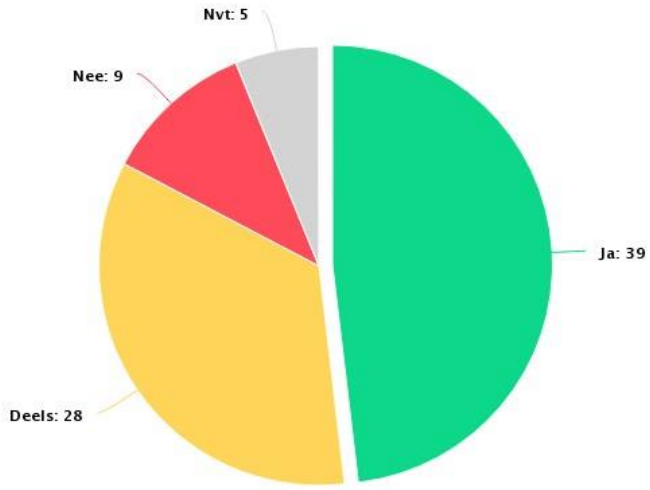
Hieronder wordt eerst de stand van zaken **einde 2022** weergegeven:

Hoofdstukken	Aantal normen	% Score
1 Privacybeleid	4	63%
2 Privacymanagement	27	66%
3 Personeel en privacy	8	67%
4 Privacy services	14	79%
5 Verwerkersovereenkomsten	4	50%
6 Verwerkingsregister	4	88%
7 Privacy compliance op verwerkingsniveau	6	17%
8 DPIA's op verwerkingsniveau	6	83%
9 Informatiebeveiliging	8	75%
Totaal	**81**	**67%**



Meting over het jaar 2021

Hieronder de resultaten van de meting aan het einde van **2021**:



2.2 Conclusie over de voortgang in 2022

Gezien de metingen is er vanaf 2021 en nu ook in 2022 een goede en stabiele situatie ontstaan. De overall-score is van 70% in 2021 naar 67% in 2022 gegaan. Op 2 normen van de 76 normen is in 2022 iets slechter gescoord. Vasthouden aan dit niveau is goed en kost ook inzet en inspanning. De normen waar nog niet aan worden voldaan betreffen vooral het onderwerp datalekken, het niet tijdig en voldoende betrokken worden op het juiste niveau, op procesniveau aandacht voor de bescherming van gegevens en de afspraken met derden en in samenwerkingsverbanden. Het volwassenheidsniveau is voldoende, maar kan vanzelfsprekend omhoog. Dat vraagt om meer inzet en aandacht op alle niveaus.

Uitgelicht over 2022:

- de bewustwording onder vooral nieuwe medewerkers is gegroeid doordat er 20 keer voorlichting gegeven is;
- er komen veel advies-vragen van medewerkers uit de organisatie; dat betekent dat de bewustwording en aandacht voor het onderwerp privacy op de werkvloer goed is;
- de DPIA-werkgroep draait zeer goed;
- de rechten van betrokkenen worden binnen de wettelijke termijnen goed verzilverd.

Onderwerpen waar meer aandacht aan besteed kan en moet worden:

- bewustwording en eigenaarschap op management- en directieniveau;
- compliance op verwerkings- en procesniveau;
- onafhankelijke positionering van de medewerkers die zich bezig houden met informatiebeveiliging en privacy;
- privacy by design: tijdig betrokken en geïnformeerd worden bij projecten en ideeën waarbij persoonsgegevens worden verwerkt;
- beleid.

In het jaarplan voor 2023 zullen deze onderwerpen verwerkt worden.

De belangrijkste constateringen over 2022 zijn:

1. Bewustwording bij de medewerkers blijft de belangrijkste pijler in de bescherming van gegevens. In 2022 is veel energie gestoken in het geven van voorlichtingen. In het jaar 2022 zijn er 20 bijeenkomsten georganiseerd. 16 daarvan waren bestemd voor de medewerkers die de afgelopen jaren in dienst zijn getreden. Door Corona konden deze collega's eerdere niet live geschoold worden op het moment van indiensttreding, maar in 2022 hebben zij meerdere kansen gekregen voor het volgen van een voorlichting. Van de 266 nieuwe collega's heeft ongeveer 50% hier gebruik van gemaakt. Daarnaast zijn 4 keer teamgerichte voorlichtingen geweest bij onder andere het KCC en bij team vergunningen.
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, maar aanzienlijk minder dan in het jaar 2021. 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 2022 is hiermee begonnen, maar in 2023 behoeft dit onderdeel verdere aandacht en uitwerking.
5. In het jaar 2021 en 2022 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. 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 en de teamleiders voor gezorgd dat voldaan werd aan de verplichtingen op basis van de Wpg. Ook in 2022 is dit weer gebeurd. Het onderwerp is echter nog niet voldoende belegd in de organisatie en er wordt op

deze manier niet voldaan aan de wettelijke eisen. Dit dient in 2023 structureel vorm gegeven te worden.

7. Beleidsstukken in het kader van privacy bieden naast het wettelijke kader de basis voor de gemeente om op te acteren. In 2022 zijn nog niet alle benodigde stukken gereed gekomen. Voor 2023 staan daarom de volgende beleidsstukken op de agenda: Privacy in het sociaal domein en Algemeen privacybeleid.
8. Er is gebleken dat regelmatig niet gebruik wordt gemaakt van Cryptshare, de tool voor beveiligd mailen met externen, terwijl dat wel wettelijk voorgeschreven is.

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 2022 heeft de gemeente Súdwest-Fryslân 16 datalekken (in 2021 waren dat er 26) gehad die bij de Functionaris gegevensbescherming zijn gemeld en daarvan zijn er vervolgens 2 gemeld bij de Autoriteit Persoonsgegevens. In 8 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, net als in 2021, de meest voorkomende oorzaak van de datalekken in onze gemeente)
- Er zijn gegevens (telefoon, dossiers) kwijtgeraakt
- Intern of extern onbevoegde toegang tot persoonsgegevens (aantal incidenten stijgt)
- Cybercrime gerelateerde gebeurtenissen

Het is niet duidelijk waardoor het aantal meldingen in 2022 behoorlijk gedaald is. Van belang is dat iedere medewerker een datalek kan herkennen, zich houdt aan de afspraken en er vertrouwen in heeft om te melden. Dit onderwerp vraagt extra aandacht in 2023 die vooral in de voorlichtingen tot uiting kan komen. Datalekken die aan de Autoriteit Persoonsgegevens en/of de betrokkenen moeten worden gemeld zijn ook in 2022 binnen de termijnen afgehandeld.

2.4 Rechten van betrokkenen

Mensen hebben verschillende rechten om contrôle 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 2022 zijn de volgende verzoeken afgehandeld:

- Verzoek tot recht op inzage: 12
- Verzoek tot verwijdering: 2
- Verzoek tot rectificatie: 0

De afhandeling heeft steeds binnen daarvoor geldende termijn plaatsgevonden.

Er zijn daarnaast 2 klachten en 5 bezwaarschriften ingediend betreffende de uitvoering van de Avg.

Er loopt 1 bezwaarprocedure bij de Autoriteit Persoonsgegevens. Een inwoner is tegen een door de Autoriteit Persoonsgegevens ongegrond verklaarde klacht, tegen onder andere de gemeente Súdwest-Fryslân, in bezwaar gegaan.

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 2022 een DPIA op is uitgevoerd zijn:

- **Automatische inkomstenverrekening**: Inwoners met een uitkering op basis van de Participatiewet of een IOAW uitkering (Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers) dienen een wijziging in hun inkomsten tijdig door te geven. De nieuwe tool zorgt voor het automatisch laten verlopen van de flexibele inkomstenverrekeningen: het berekenen van de juiste uitkering zonder een menselijke tussenkomst. Via het invullen van een slim formulier wordt een berekening gemaakt van de juiste inkomstengegevens.

- **Bibobscan**: tooling die wordt gebruikt voor de Bibob-scan: het gebruik van de Bibob-scan is ontwikkeld door Web-IQ (IRIS). Dit is een instrument dat is ontwikkeld waarmee bovenstaande onderwerpen sneller en beter gescand kunnen worden in de Bibob toetsing dan nu het geval is. Deze tool gaat op basis van door de eindgebruiker ingevoerde data real-time op zoek naar informatie op het open internet. De verandering ten opzichte van de huidige situatie is dat het Bibob onderzoek nu geen digitaal proces kent: de Bibob toetsing werd handmatig uitgevoerd door middel van het zoeken in openbare bronnen.
- **Tachograaf:** ingebruikname van een op afstand digitaal uit te lezen tachograaf. Hierdoor kunnen de tachografen op afstand digitaal uitgelezen worden in enkele seconden in plaats van dat deze handmatig uitgelezen moeten worden.
- **Xential/vervanging documentatie-creatiesysteem**: Het in gebruik nemen van een nieuw documentcreatiesysteem. Het is voor de dienstverlening van de gemeente van groot belang dat via sjablonen brieven in een standaard formaat worden opgemaakt. Dit om uniform te kunnen communiceren met burgers/bedrijven (waarborgen van de kwaliteit van uitgaande documenten) en ter vereenvoudiging van interne processen.

Van start gegaan in 2022 en bijna afgerond:

- Gegevensmagazijn sociaal domein

3. Jaarplan 2023

De meting over 2022 geeft duidelijk weer welke normen nog geïmplementeerd dienen te worden of waar verder versterkt kan worden. Voor het jaar 2023 is gekozen voor in ieder geval de volgende acties en aandachtspunten:

1. **Beleid:**

- Algemeen privacy-beleid herschrijven.
- Beleid privacy in het sociaal domein wordt vastgesteld. In het sociaal domein wordt, onder andere door het gebruik van de brede vraagverheldering, deels buiten de fingerende wetgeving gewerkt. Omdat het Sociaal Domein (op sommige punten) afwijkt van de Avg of materiewetten dient beschreven en vastgesteld te worden in beleid waarom dat gebeurt en op welke wijze. Op die manier wordt recht gedaan aan de eisen van transparantie en accountability.

2. **Privacymanagement**

- Verantwoordelijkheden en taken voortkomend uit de Wet Politie Gegevens beleggen. (zie bladzijde
- Teamleiders zijn (eind-) verantwoordelijk voor de verwerkingen van persoonsgegevens binnen hun team.
- Eigenaarschap management: Informatiebeveiliging en gegevensbescherming staan op de managementagenda. Uitvoering bedenken om vorm te geven aan succesfactor 3 van de IBD[1].
- 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.
- Rol van ethiek inbedden in (privacy-)adviezen en wegingen. Ethische afwegingen mee laten wegen bij de inzet van een nieuwe technologie en het gebruik van data in de openbare ruimte of publieke dienstverlening (voorbeelden: inzet bodycams, sensoren in de stad, scanauto's parkeren, datagedreven werken, robotisering). Gebruik van nieuwe technologie en inzet op digitalisering kan raken aan de vraag wat voor samenleving we willen zijn. Het gaat hier niet om vragen over effectiviteit en efficiency, maar om de zoektocht naar de publieke waarden die worden nagestreefd. Zeer actueel onderwerp waar veel gemeentes al stappen in hebben gemaakt.

3. **Personeel en privacy**

- Gezamenlijk blijven optrekken in het kader van bewustwording met de CISO die gaat over de Informatiebeveiliging.
- Organisatie: onafhankelijker positionering van de Chief Information Officer (CISO), Functionaris gegevensbescherming (FG), Privacy Officer (PO) en een veilige

1 https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

cultuur. De functies zijn verdeeld over verschillende teams. Positionering heroverwegen in kader van efficiëntie en onafhankelijkheid. Succesfactor 4 van de IBD[2].
- Voorlichting blijven verzorgen voor nieuwe medewerkers. De voorlichting verplicht stellen zodat iedereen weet hoe veilig en zorgvuldig te werken met gegevens. Actief zijn bij het on-boarden. Succesfactor 6 van de IBD.

4. Privacy services

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

5. Overeenkomsten met derden (gezamenlijke verantwoordelijken) en verwerkers

- Alle samenwerkingsverbanden worden in kaart gebracht en dienen te voldoen aan de Avg. Succesfactor 5 van de IBD: *Samenwerkingsverbanden:* maak afspraken en zie erop toe[3].

6. Verwerkingsregister

- Bijhouden. Geen extra acties nodig.

7. Privacy compliance op verwerkingsniveau

- Privacy by design versterken: tijdig betrekken bij projecten en ideeën waarbij persoonsgegevens worden verwerkt;

8. DPIA's

- Voortzetting uitvoeren van DPIA’s.

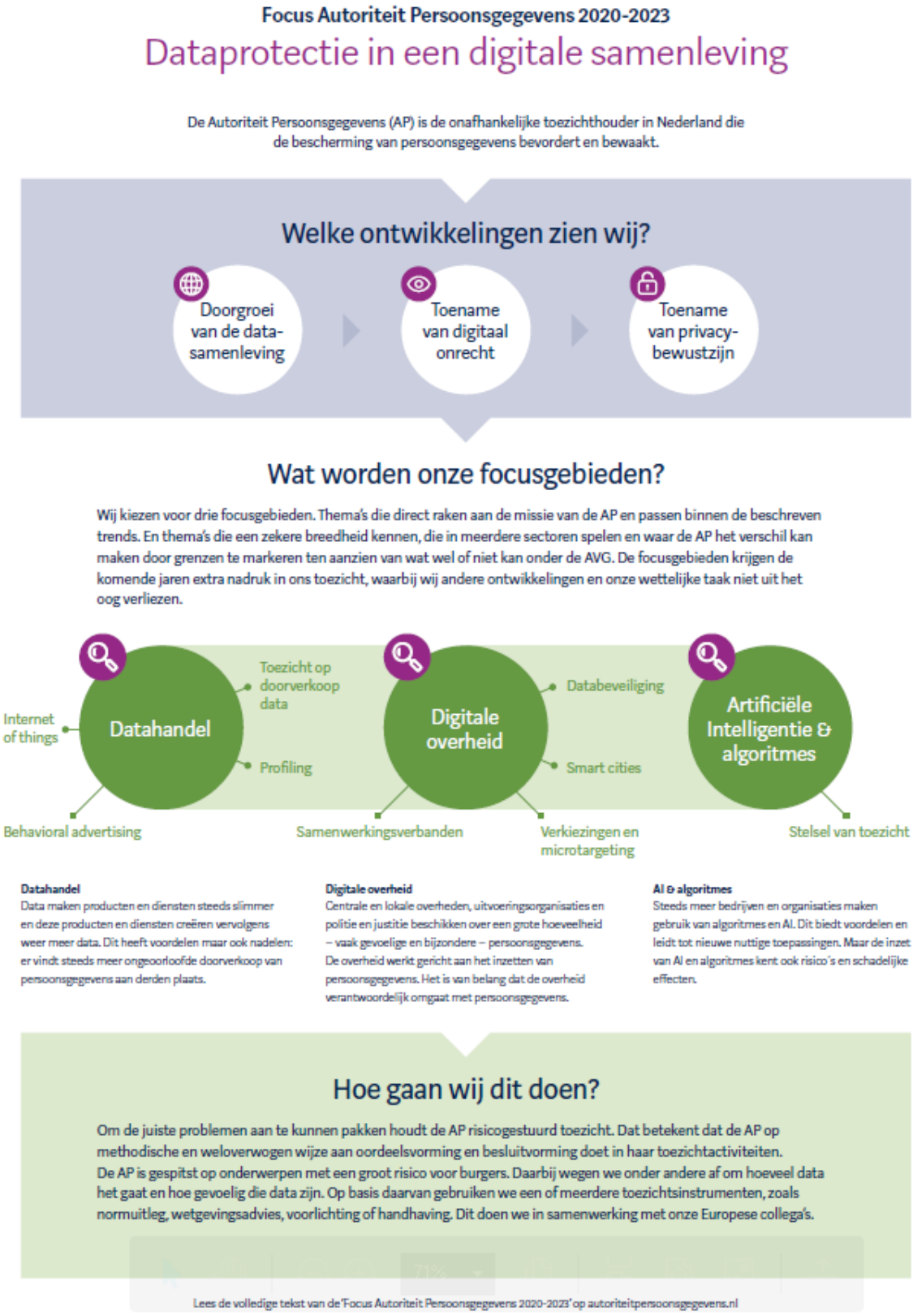
9. Informatiebeveiliging

- Samenwerking met CISO en ISO en Integriteits-coördinatoren continueren.
- Gezamenlijk met Juridische en Veiligheidszaken (JVZ), CISO en FG een Cybersecurity-crisisplan opstellen.

2 https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

3 https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

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 voor-lichting, 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

71%