Rapportage informatieveiligheid en privacy

Periode 2024

Gemeente Ooststellingwerf

Datum :14-04-2025

Auteur: Hans Siccama

Inhoudsopgave

1 Versiebeheer

Versie	Datum	Opsteller	Te versturen aan
1.0	30-04-2018	Hans Siccama	MT, College van B&W en Raad
2.0	01-05-2019	Hans Siccama	MT, College van B&W en Raad
3.0	06-05-2020	Hans Siccama	MT, College van B&W en Raad
4.0	06-05-2021	Hans Siccama	MT, College van B&W en Raad
5.0	04-05-2022	Hans Siccama	MT, College van B&W en Raad
6.0	02-05-2023	Hans Siccama	MT, College van B&W en Raad
7.0	02-05-2024	Hans Siccama	DT, College van B&W en Raad
8.0	xx-04-2025	Hans Siccama	DT, College van B&W en Raad

2 Verantwoording

De rapportage wordt jaarlijks opgemaakt door de beveiligingsfunctionaris (CISO) / functionaris gegevensbescherming (FG) en ter kennisname verstuurd aan de directie, B&W en gemeenteraad. De gemeenteraad wordt tevens over de status van informatiebeveiliging en privacy geïnformeerd in de paragraaf bedrijfsvoering als onderdeel van de jaarstukken.

3 Doel en scope

Deze jaarrapportage bevat de ontwikkelingen, activiteiten, incidenten en risico's met betrekking tot de onderwerpen informatieveiligheid en privacy bij de gemeente Ooststellingwerf over het jaar 2024. Het geeft een beeld van de trends en de bedreigingen die van invloed zijn of kunnen zijn op de gemeente. De rapportage is in overeenstemming met het door het college vastgestelde informatiebeveiligingsbeleid en is uitgebreid met het aandachtsgebied Privacy ten aanzien van de bescherming van persoonsgegevens in het kader van de Algemene Verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

4 Beleid en verantwoording

4.1 Beleid

In het gemeentelijke informatiebeveiligingsbeleid, laatstelijk door het college vastgesteld op 5 december 2023, en geldend voor een periode van 3 jaar, is de Baseline Informatiebeveiliging Overheid (BIO) opgenomen. Deze richtlijn, algemeen aanvaard als normenkader, bevat een totaalpakket aan informatiebeveiligingsmaatregelen geldend voor elke gemeente. Alle normen die gelden voor de specifieke wetgeving (o.a. PUN, RR, BRP, Suwi, DigiD, BAG, BGT en BRO) zijn hierin grotendeels geïntegreerd.

Met de vaststelling van het algemene informatiebeveiligingsbeleid, de verantwoordelijkheden en de normen voor de informatiebeveiliging stelt het college de kaders voor informatiebeveiliging vast (volgens de BIO-norm tenminste om de 3 jaar opnieuw of eerder indien grote wijzigingen). In de verantwoordelijkheden is opgenomen dat het onderliggende, flankerende beleid inclusief procedures, richtlijnen en beveiligingsmaatregelen vastgesteld worden door de directie.

Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy zowel intern binnen onze eigen organisatie als naar de burger toe. De gemeente geeft middels beleid een duidelijke richting aan privacy en laat daarmee zien dat zij de privacy waarborgt, beschermt en handhaaft. Daarnaast heeft de gemeente privacybeleid ontwikkeld specifiek voor onze burgers. Dit beleid samen met de privacyverklaring is gepubliceerd op onze gemeentewebsite. Het beleid hoe wij intern binnen de gemeente omgaan met privacy en het beleid specifiek voor onze inwoners is voor het eerst conform de AVG vastgesteld in 2018 en wordt eens in de 4 jaar (raadsperiode) herzien.

De Wet politiegegevens (Wpg)
Wanneer een gemeente haar taken uitvoert en daarbij persoonsgegevens verwerkt, is de Algemene Verordening Gegevensbescherming (AVG) altijd van toepassing echter als een buitengewoon opsporingsambtenaar (boa) persoonsgegevens verwerkt, dan ligt dat soms net even anders. Die gegevens kunnen namelijk onder verschillende wettelijke regimes vallen.

Er zijn zes werkterreinen, ook wel domeinen genoemd, waarop boa's actief zijn:
• De openbare ruimte (o.a. handhavers, parkeerwachters, bouw en woningtoezicht, controleurs).
• Het milieu, welzijn en infrastructuur (o.a. groene Boa's, boswachters, jachtopzieners, milieu-inspecteurs, waterinspecteurs, weginspecteurs).
• Het onderwijs (leerplichtambtenaren).
• Het openbaar vervoer (conducteurs, BOA-OV).
• Werk, inkomen en zorg (o.a. sociaal rechercheurs, arbeidsinspectie, belastingcontroleurs en -inspecteurs).
• Generieke opsporing (boa's bij politie).

AVG versus Wpg
Persoonsgegevens die een boa verwerkt in zijn rol als toezichthouder (toezichts- en handhavingstaken) vallen onder de AVG. Sinds 2019 mogen buitengewoon opsporingsambtenaren (boa's) ook politiegegevens verwerken in het kader van opsporing van strafbare feiten. Het verwerken van dit type gegevens valt niet onder de Algemene Verordening Gegevensbescherming (AVG), maar onder de Wet politiegegevens (Wpg).

Voor gegevens die onder de Wpg worden verwerkt (voor opsporing dus), gelden andere regels dan onder de AVG zoals bijvoorbeeld ten aanzien van bewaartermijnen of eisen die gelden bij het onderling delen van gegevens. Het is daarom van belang dat de gegevensverwerkingen die onder de Wpg vallen, andere kenmerken krijgen dan de gegevensverwerkingen die onder de AVG vallen.

Activiteiten gericht op opsporing valt dus onder de WPG, maar op toezichts- en handhavingstaken is de AVG van toepassing. Een boa heeft bij het verwerken van persoonsgegevens zowel met de AVG te maken als met de Wpg. In deze verwerking van gegevens moet duidelijk zijn welke gegevens er specifiek worden verwerkt onder de AVG en welke onder de Wpg.

Nieuw privacybeleid
Op grond van de Wet op de ondernemingsraden heeft de OR instemmingsrecht over het privacybeleid voor zover het interne toezicht de gegevensbescherming van het personeel raakt. De OR is derhalve om instemming gevraagd om de Wet politiegegevens te integreren in het gehele privacybeleid en aan te vullen in de taken, verantwoordelijkheden en bevoegdheden zoals deze zijn vastgelegd in het Reglement Functionaris voor de gegevensbescherming. Dit geheel is op 29 november 2022 door het college vastgesteld. Ook het privacybeleid en de privacyverklaring zoals dat op onze gemeentewebsite is gepubliceerd is geactualiseerd en vastgesteld door het college op 7 maart 2023.

De indiener van dit rapport en Rowena van der Veen zijn formeel aangewezen als Functionaris Gegevensbescherming voor de AVG en voor de Wpg. Beide zijn als contactpersoon aangemeld bij de Autoriteit Persoonsgegevens (AP).

4.2 ENSIA

Wat is ENSIA?
ENSIA staat voor Eenduidige Normatiek Single Information Audit en betekent eenmalige informatieverstrekking en eenmalige IT-audit.

ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen.

Horizontale verantwoording

Met ingang van 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) in werking getreden. Hiermee is er voor alle overheidslagen (Rijk, provincies, waterschappen en gemeenten) één gezamenlijk normenkader gerealiseerd. Deze baseline is de kern van de verantwoording over informatieveiligheid aan de gemeenteraad. De horizontale verantwoording bestaat uit de zelfevaluatie, een IT-audit, een verklaring van het College van B&W, een jaarlijkse rapportage (voorliggend) en een passage over informatieveiligheid en privacy in de paragraaf bedrijfsvoering.

Verticale verantwoording

Over de BRP, PNIK, Suwinet, DigiD, BAG, BGT en BRO moeten gemeenten ook verantwoording afleggen. Dit noemen we de ‘verticale verantwoording’. De horizontale verantwoording richting gemeenteraad vormt hiervoor de basis. De normen van de BIO en de specifieke normen van de BRP, PNIK, Suwinet, DigiD, BAG, BGT en de BRO zijn opgenomen in de zelfevaluatievragenlijst.

Single Information Audit

Uitgangspunt van ENSIA is de single information audit. Dit betekent dat maar één keer per jaar de zelfevaluatielijst ingevuld hoeft te worden. Deze informatie wordt gebruikt voor de horizontale verantwoording richting gemeenteraad en de diverse verticale verantwoordingslijnen richting de departementen en toezichthouders.

Organisatie

Om het verantwoordingsproces voorspoedig te laten verlopen, heeft de gemeente een coördinator ENSIA aangewezen voor het begeleiden, bewaken en waar nodig bijsturen van het verantwoordingsproces. De lijn blijft verantwoordelijk voor de inhoud en/of het resultaat van de audit. De beveiligingsfunctionaris (CISO) is aangewezen als coördinator ENSIA. Deze stelt jaarlijks een plan van aanpak op. Dit plan van aanpak geeft inzicht in de uit te voeren acties in het verantwoordingsproces en de rol daarin van de ENSIA-coördinator en wordt vastgesteld door de directie.

<u>Vragenlijst zelfevaluatie Informatieveiligheid</u>
De zelfevaluatie over informatieveiligheid over de volle breedte van de BIO en specifieke domeinen wordt uitgevoerd door middel van het beantwoorden van vragenlijsten in de online ENSIA-tool. Met de ingevulde zelfevaluatie vragenlijst en bijbehorende rapportages geeft het college van B&W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen.

De scope van de IT-audit over verantwoordingsjaar 2024 heeft betrekking op DigiD en SUWI. De verantwoording Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) vindt plaats door middel van een Collegeverklaring. De Collegeverklaring is opgesteld op basis van de bevindingen uit onze zelfevaluatie en is getoetst door een onafhankelijke IT-auditor.

De Collegeverklaring ENSIA 2024 omvat het op 31 december 2024 voldoen van de beheersmaatregelen in opzet en bestaan en bij een aantal normen ook de werking inzake DigiD en Suwinet.

Deze toets op de werking bij een aantal normen inzake DigiD vindt voor het eerst plaats over het verantwoordingsjaar 2024. Met ingang van het verantwoordingsjaar 2026 zal de toets op de werking van normen ook onderdeel uit gaan maken voor wat betreft Suwinet.

Uit de Collegeverklaring ENSIA blijkt dat aan alle normen m.b.t. de DigiD-aansluitingen en Suwinet wordt voldaan. Aanbevelingen welke zijn opgenomen in de onderliggende rapportages van bevindingen zijn derhalve niet dwingend van aard en zullen met de verantwoordelijken worden besproken waarbij op basis van risico-inschatting een afweging zal worden gemaakt of het noodzakelijk is eventuele maatregelen te treffen.

Baseline informatiebeveiliging overheid (BIO)

Met de inwerkingtreding van de Baseline Informatiebeveiliging Overheid (BIO) is er voor alle overheidslagen (Rijk, provincies, waterschappen en gemeenten) één gezamenlijk normenkader gerealiseerd. Deze baseline is de kern van de verantwoording over informatieveiligheid aan de gemeenteraad.

De BIO legt de nadruk op risicomanagement. Om hieraan invulling te kunnen geven is tegelijkertijd met de BIO de handreiking ‘10 bestuurlijke principes voor informatiebeveiliging’ van kracht. Deze principes ondersteunen bestuurders bij de invulling van hun verantwoordelijkheid.

Kenmerken van de BIO:

1. Maatregelen zijn altijd verplicht
2. Gericht op risicomanagement (het begint met een QuickScan)
3. Er zijn 3 Basisbeveiligingniveaus (BBN)
4. Selectie van ontbrekende maatregelen vooraf
5. Toewijzing van maatregelen op eindverantwoordelijke
6. Een baselinetoets (QuickScan) die rekening houdt met die 3 niveaus

De Informatiebeveiligingsdienst (IBD) ondersteunt gemeenten daarbij met producten en regionale bijeenkomsten.

Stappenplan per informatiesysteem:

1. Informatiesystemen bekend en eigenaarschap vastgelegd
2. Baselinetoets en niveau vastleggen (BBN-analyse)
3. (Diepgaande) Risicoanalyse / -afweging (optioneel)
4. Registratie toepasselijkheid maatregelen voor informatiesysteem
5. GAP-analyse maatregelen door proceseigenaar
6. Selectie en toewijzing van controls & maatregelen aan eigenaar
7. Implementatie en borging maatregelen door proceseigenaar
8. Monitoring status via ISMS (kwaliteitsmanagementsysteem Informatiebeveiliging), periodieke rapportages en bijstellen.

Definitie informatiesysteem:
“… een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerkingen communicatie.”

Implementatie in de praktijk:
De beveiligingsfunctionaris (CISO) vervult in de hierboven genoemde stappenplan een coördinerende rol, e.e.a. voor wat betreft de samengevoegde OWO onderdelen ook in samenwerking met de beveiligingsfunctionarissen van Weststellingwerf en Opsterland.

Het huidige informatiebeveiligingsbeleid is gebaseerd op de BIO. Door middel van een GAP-analyse is samen met de verantwoordelijken in de procesgang bezien welke maatregelen vervolgens in het kader van de BIO verplicht zijn om door te voeren. De implementatie van de BIO vindt gefaseerd plaats, met risicobeheersing als belangrijkste doel, op basis van onderstaande volgorde:

1. Gemeentebrede informatiebeveiliging:

   De gemeente dient passende technische en organisatorische beveiligingsmaatregelen te treffen. Het treffen van technische beveiligingsmaatregelen is vooral een verantwoordelijkheid van I&A; het treffen van organisatorische beveiligingsmaatregelen heeft vooral betrekking op het werkveld van HRM (beveiligingsmaatregelen m.b.t. personeel) en Dienstverlening ((voorheen Beheer en Onderhoud) (beveiligingsmaatregelen m.b.t. de gebouwen)).

2. Risicovolle informatiesystemen:

   In lijn met het borgen van de privacy met de systemen waarin bijzondere persoonsgegevens of anderszins van gevoelige aard worden verwerkt en waarvoor specifieke normen gelden. Dit betreffen de processen binnen: Jeugd, WMO, Participatie, Openbare Orde en Veiligheid, Burgerzaken, BVI, Financiën, Salarissen, VTH.

3. Overige informatiesystemen:

   Processen waarin enkel algemene persoonsgegevens (o.a. naam, adres, woonplaats, emailadres) worden verwerkt. Hier lopen we gezien de aard van de gegevens minder risico.

Ontwikkelingen 2025
Er wordt gewerkt aan een nieuwe kader voor de overheid voor informatiebeveiliging, de BIO2. Met de BIO2 wordt tevens invulling gegeven aan eisen vanuit de NIS2-richtlijn, die horen bij de beveiliging van overheidsinformatie. De NIS2 is een nieuwe Europese richtlijn gericht op het vergroten van digitale weerbaarheid en het beperken van de gevolgen van cyberincidenten in de Europese Unie (EU). In de richtlijn is hiertoe onder meer een zorgplicht en een meldplicht opgenomen. De NIS2 richtlijn is niet rechtstreeks van toepassing op gemeenten, maar wordt uitgewerkt in de Cyberbeveiligingswet, waar gemeenten wel aan moeten voldoen. Naar verwachting wordt de wet in het derde kwartaal van 2025 ingevoerd. Vanaf het moment dat de wet ingaat, moet de gemeentelijke digitale veiligheid voldoen aan de eisen die in deze wet staan.

Op basis van de BIO2 zal wederom door middel van een GAP-analyse worden bezien, welke maatregelen vervolgens in het kader van de BIO2 verplicht zijn om door te voeren, waarbij nagenoeg het zelfde stappenplan als hierboven is aangegeven, zal worden doorlopen. Het principe van de basis beveiligingsniveau's (BBN's) zal daarbij wel worden worden losgelaten. De BIO2 hanteert een nog meer risicogebaseerde aanpak. De BIO2 zal worden verankerd in de Cyberveiligheidswet.

4.3 Informatiebeveiligings- en privacybewustzijn

Informatie is één van de voornaamste bedrijfsmiddelen van Ooststellingwerf. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging is het proces dat dit belang dient.

Visie

De komende jaren zet de gemeente Ooststellingwerf in op het verhogen van informatieveiligheid en

verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven.[1] Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Door gebrek aan informatiebeveiligings- en privacybewustzijn en het ontbreken of in ieder geval niet volgen van maatregelen om de informatieveiligheid en privacy te borgen, loopt de gemeente het risico op hoge boetes in het kader van de Algemene Verordening Gegevensbescherming (AVG), Wet politiegegevens (Wpg), schadeclaims bij datalekken en op imagoschade (vertrouwen burger/media).

Informatieveiligheid is een verantwoordelijkheid van heel de organisatie. Hoe goed de techniek ook is georganiseerd, als medewerkers de deuren open houden voor vreemden, slordig omgaan met wachtwoorden of bijvoorbeeld phishingmail niet herkennen, dan blijft de informatieveiligheid zeer kwetsbaar.

Met het oog op deze visie en het voldoen aan de normen inzake informatiebeveiliging en privacywetgeving zijn binnen de gemeente al eerder acties ingezet, structureel van aard, hieronder een overzicht:

1. De raad wordt structureel op de hoogte gesteld van de complexiteit van de dilemma's op het gebied van informatieveiligheid.

Ondernomen acties:
De raad wordt middels de P&C-cyclus op de hoogte gesteld van ontwikkelingen en doelen op het gebied van o.a. ICT, digitalisering en informatieveiligheid. Informatieveiligheid maakt binnen onze gemeente al jaren onderdeel uit van de paragraaf Bedrijfsvoering. Met de invoering van de AVG, per 25 mei 2018, is ook privacy toegevoegd in deze paragraaf. Ook de Wpg is hierin als nieuw onderdeel toegevoegd. De raad wordt daarnaast jaarlijks middels deze rapportage geïnformeerd.

2. Informatieveiligheid vindt plaats op basis van een planmatige aanpak en over de voortgang wordt gerapporteerd.

Ondernomen acties:
Om de drie jaar wordt het strategische informatiebeveiligingsbeleid, kaderstellend en richtinggevend, geactualiseerd en door het college vastgesteld. Onderliggend, flankerend beleid inclusief procedures, richtlijnen en beveiligingsmaatregelen waarop specifieke wetgeving van toepassing is, worden jaarlijks vastgesteld door de directie. Op basis van het oude informatiebeveiligingsbeleid, gebaseerd op de BIG en vastgesteld d.d. 7 februari 2017, heeft er al een GAP- en impactanalyse plaatsgevonden, met als resultaat dat we inzicht hebben in de status van informatiebeveiliging, actiehouders en planning. De uitkomsten hiervan zijn na afloop van het verantwoordingsjaar 2018 verwerkt in de zogenaamde Verklaring van Toepasselijkheid (VVT) en op 11 juni 2019 door het college van B&W vastgesteld. Met het vaststellen van de VVT doet het college een uitspraak welke beveiligingsmaatregelen we gaan nemen en welke maatregelen we bewust/weloverwogen niet nemen (aanvaardbaar risico). Hiermee is er een basis gelegd.

Ook in het kader van de inwerkingtreding van de BIO is er daarna door middel van een GAP- en impactanalyse bezien welke maatregelen ten opzichte van de vervangen Baseline Informatiebeveiliging Gemeenten (BIG) nog moeten worden geimplementeerd. Ontwikkelingen op landelijk niveau welke eventueel leiden tot een nieuw normenkader en eventueel nieuwe te treffen maatregelen worden hierin meegenomen. Dit is een continu proces. Het treffen van passende technische en organisatorische beveiligingsmaatregelen om daarmee volledig te voldoen aan de BIO kan niet in één keer. De implementatie van deze maatregelen in het kader van de BIO vindt derhalve gefaseerd plaats, op basis van risicoinschatting, capaciteit en beschikbare middelen.

[1] Met betrouwbare informatievoorziening wordt bedoeld dat de volgende zaken geregeld zijn: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.

Cyberalert
Een betrouwbare en veilige overheid vraagt om gedegen beveiliging van de informatie en bescherming van de privacy binnen de gemeentelijke informatiehuishouding. Inwoners vertrouwen ons immers hun identiteit- en persoonsgegevens toe. Veel incidenten kunnen voorkomen worden door het 'eigen huis op orde' te hebben en te houden. Dat vraagt om permanente en bestuurlijke aandacht. Als gevolg van de toenemende digitale dienstverlening neemt ook de kans op cybercrime toe.

De VNG/IBD heeft in 2021 een dringende oproep aan alle burgemeesters in Nederland gedaan om met college, raad en ambtelijke organisatie de benodigde tijd, mensen en middelen vrij te maken om de digitale beveiliging van gemeenten in lijn te brengen met de actuele risico's van cybercrime. De VNG/IBD adviseert in dit kader de navolgende maatregelen met de hoogste prioriteit in te voeren en bij te houden:

1. Houd hard- en software up-to-date
2. Gebruik meerfactorauthenticatie
3. Hanteer een strikte netwerksegmentatie
4. Zorg voor robuuste backups
5. Test en oefen uw ICT-crisisplan(nen)

Digitale Veiligheid: kerntaak van gemeenten
Met deze oproep benadrukt het VNG-bestuur het belang van digitale weerbaarheid. In de Algemene ledenvergadering van februari 2021 is de resolutie 'Digitale veiligheid: kerntaak voor gemeenten' unaniem aangenomen.

De resolutie bevat 9 concrete actiepunten voor gemeenten:
1. Structureler incidenten delen met elkaar en met andere sectoren via de IBD.
2. Jaarlijks een incidentoverzicht op categorieniveau delen met de IBD, zodat een compleet inzicht bestaat in dreigingen, trends en ontwikkelingen.
3. Elk jaar een digitaal incidentbestrijdingsplan actualiseren en vaststellen.
4. Elkaar helpen bij digitale incidenten en de nasleep daarvan.
5. Periodiek oefenen met cyberincidenten om de gemeentelijke weerbaarheid te toetsen en te vergroten.
6. Het onderwerp digitale veiligheid periodiek in het college van B&W bespreken.
7. Digitale risico's opnemen in de Integrale Veiligheidsplannen.
8. Structureel voldoende budget vrijmaken voor blijvende weerbaarheid tegen digitale dreigingen (naar advies van de CyberSecurityRaad).
9. Waar mogelijk gebruik maken van de gezamenlijk ontwikkelde voorzieningen en programma's die zich richten op digitale veiligheid.

De hierboven genoemde prioriteiten zijn onderdeel van het normenkader voor de Nederlandse overheid, de Baseline Informatiebeveiliging Overheid (BIO). Hierin zijn ook normen opgenomen die betrekking hebben op het verhogen van de digitale weerbaarheid binnen gemeenten. Digitale veiligheid staat binnen OWO derhalve continu op de agenda.

De afgelopen jaren zien we dat verschillende ontwikkelingen de veiligheid van onze maatschappij en economie steeds meer onder druk zetten. Er is een verschuiving gaande van fysieke openbare orde naar digitale openbare orde.

Team OOV houdt zich bezig met de lokale openbare orde en veiligheid. Ook digitale veiligheid van inwoners en ondernemers valt hieronder. Daar waar OOV een rol speelt in de digitale veiligheid voor/van de inwoner, speelt de CISO een rol bij de digitale (informatie)beveiliging/veiligheid van de organisatie. Er is dan wel een vlak waar dit elkaar raakt: bij cyberincidenten of –crisissen. Dit heeft gevolgen voor de eigen organisatie, maar kan ook gevolgen hebben voor de inwoner. Binnen onze gemeente werken OOV en de CISO daarom nauw met elkaar samen.

Cybercrime kan de samenleving ontwrichten. Ondanks het sterke grensoverschrijdende karakter van cybercrime en gedigitaliseerde criminaliteit heeft de gemeente een belangrijke rol in het voorkomen

van lokaal slachtoffer- en daderschap. De gemeente is de aangewezen instantie om verschillende partijen bij elkaar te brengen in de preventie van cybercrime en gedigitaliseerde criminaliteit.

In de lokale aanpak van cybercriminaliteit kunnen wij als gemeente gebruik maken van het ondersteuningsprogramma van de VNG en Centrum voor Criminaliteitspreventie Veiligheid (het CCV); dit is een onafhankelijke stichting die helpt veiligheidsproblemen in kaart te brengen en op te lossen. Hiervoor bieden ze kennis, instrumenten, keurmerken, voorlichtingsmateriaal en advies op maat gericht op veilig wonen, veilig werken en veilig leven. Preventie is daarbij steeds het uitgangspunt.

3. Er wordt aandacht besteed aan leveranciersmanagement.

Ondernomen acties:
Bij de aanschaf van systemen is het belangrijk vooraf informatiebeveiligings- en privacyaspecten in het eisenpakket mee te nemen en - ingeval van het verwerken van persoonsgegevens - op te nemen in verwerkersovereenkomsten. Dit is in 2018 daarom al doorgevoerd als onderdeel van het startformulier in het inkoopbeleid.

De samenwerking tussen de drie gemeenten is bekrachtigd in de bestuursovereenkomst OWO. Ter aanvulling is er tussen de drie samenwerkende gemeenten de regeling gezamenlijke verantwoordelijkheid opgesteld en op 17 september 2018 door de afzonderlijke colleges vastgesteld.

Met de invoering van de Algemene Verordening Gegevensbescherming (AVG) zijn de eisen waaraan verwerkingen van persoonsgegevens moeten voldoen verscherpt. Onze gemeente beschikt sindsdien over een privacy verwerkingsregister, centraal bijgehouden door de Functionaris Gegevensbescherming (FG). In dit register worden ook verwerkingen opgenomen die zijn uitbesteed aan leveranciers. Met ingang van het jaar 2023 is er ook in het kader van de Wet politiegegevens (Wpg) een verwerkingsregister opgesteld.

4. Leercirkel I-bewustzijn.

Ondernomen acties:
De leercirkel I-bewustzijn is met ingang van 2016 voor de gemeente de basis om het informatiebeveiligingsbewustzijn (en met ingang van het jaar 2018 ook de privacybewustzijn) binnen de organisatie op een hoger niveau te brengen en te houden.

De cyclus bestaat uit acties in het kader van leren, begeleiden en ontwikkelen van het informatiebeveiligings- en privacybewustzijn, waarna wordt overgaan met het toetsen en beproeven ervan. Dit is een continu proces. Het uitzetten van acties om de informatiebeveiligings- en privacybewustzijn binnen de organisatie continu onder de aandacht te brengen behoort tot het takenpakket van de beveiligingsfunctionaris en Functionaris Gegevensbescherming (CISO en FG).

Hieronder volgt een opsomming van de acties die zijn ingezet:

- 2017: presentatie aan het college over de leercyclus;
- 2017: E-learning Ibewustzijnpakket bestaande uit 6 modules en 6 kennistesten met de mogelijkheid tot het behalen van een certificaat (behaalde deelnamepercentage 76 %) en gedurende een jaar lang de mogelijkheid terug te kijken en/of opnieuw uit te voeren;
- 2017: inzet Mystery Guest;
- 2018: plaatsen van de belangrijke uitkomsten van het bezoek van de Mystery Guest inclusief de top 10 met belangrijkste aandachtspunten op intranet;
- 2018: in het kader van de implementatie van de AVG hebben er binnen de diverse afdelingen bijeenkomsten plaatsgevonden om uitleg te geven over deze wetgeving inclusief meldplicht datalekken en de gevolgen ervan voor ons als gemeente; de organisatie is tevens op de hoogte gebracht via intranet.

- 2018: kahootbijeenkomsten over de AVG inclusief meldplicht datalekken (quizvorm) aan het MT en aan een aantal specifieke afdelingen waarbinnen gevoelige persoonsgegevens worden verwerkt t.w. de Gebiedsteams, Backoffice Sociaal Domein en BVI.
- 2018: digitale opruimdag
- 2018: presentatie aan de raad.
- 2019: presentatie door SEP over informatiebeveiliging en privacy aan het college
- 2019: lunchbijeenkomst cybercrime en cybersecurity in de raadszaal, internationaal gastspreker Peter Zinn met 10 jaar ervaring als cybercop bij het Team High Tech Crime van de politie.
- 2019 met doorloop 2020: E-learning Privacy (3 modules) en datalekken (1 module) voor de gehele organisatie inclusief raadsleden met de mogelijkheid tot het behalen van een certificaat (behaalde deelnamepercentage 66 %) en gedurende een jaar lang (tot 21 okober 2020) de mogelijkheid terug te kijken en/of opnieuw uit te voeren.
- 2020: plaatsing periodieke informatie op intranet voor de gehele organisatie over herkennen phishingmail, ransomware, malware, whatsappfraude.
- 2020: vakantieboekje in het kader van informatiebeveiliging en privacy: tips over veilig internetten op vakantie, afgeven kopie paspoort, pseudonimiseren en anonimiseren kruiswoordpuzzel, woordzoeker, rebus.
- 2021/2022: e-learningcampangne veilig thuiswerken, voor de gehele ambtelijke organisatie.
- 2023: presentatie aan de raad (huidige samenstelling).
- 2023: maandelijkse plaatsing informatie op intranet voor de gehele organisatie over herkennen van diverse vormen van cybercrime
- 2023/2024: wekelijks korte kennisvragen over informatieveiligheid en privacy in de mailbox (nano-learning) binnen de gehele organisatie
- 2024: phishingtest, uitgezet binnen de gehele organisatie.
- 2024: lezing cybercrime en AI door Maria Genova.
- 2024/2025: plaatsing periodieke informatie op intranet voor de gehele organisatie over herkennen phishingmail, ransomware, malware, whatsappfraude.

Informatieveiligheid en privacy zijn derhalve thema's die doorlopend aandacht verdienen. Beveiligd mailen, beveiligd printen, het instellen van een bezoekersregistratie, het plaatsen van containers met gleuf voor de afvoer van vertrouwelijke stukken zijn voorbeelden van de maatregelen die onze gemeente eerder al heeft getroffen om de kans op een datalek te verkleinen.

4.4 Waar staat je gemeente

Net als andere gemeentelijke informatie, staan de gegevens over informatieveiligheid vermeld op de website waarstaatjegemeente.nl. Hierbij kunnen gegevens tussen verschillende gemeenten worden vergeleken. Deze gegevens zijn niet alleen toegankelijk voor gemeentelijke bestuurders maar ook voor andere geïnteresseerde partijen zoals inwoners, onderzoekers en media.

5 Privacy

AVG

Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. De gemeente dient zorgvuldig om te gaan met persoonsgegevens. Bij de uitoefening van onze taken verwerkt de gemeente veel informatie. Niet alleen persoonlijke informatie van onze eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties. In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de gemeente transparant te zijn welke persoonsgegevens zij verwerkt en voor welk doel. Persoonsgegevens mogen alleen

worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor deze zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. Met de invoering van de AVG zijn de eisen waaraan verwerkingen van persoonsgegevens moeten voldoen dus verscherpt. Burgers hebben als gevolg hiervan ondermeer recht op inzage van welke gegevens worden verwerkt, maar ook het recht om gegevens uit de database te verwijderen, tenzij legitieme wettelijke vereisten dit voorkomen.

Bovendien moet de gemeente passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoonsgegevens te voorkomen. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van onze gemeente. Privacy heeft een direct raakvlak met informatiebeveiliging.

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om persoonsgegevens van eigen inwoners, inwoners van andere gemeenten, zakenrelaties, medewerkers en externen. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels.

Daarnaast dient de gemeente te beschikken over een interne toezichthouder: de Functionaris voor de Gegevensbescherming (FG). De verschillende bestuursorganen van de gemeente, t.w. het college van B & W, de burgemeester, de raad van de gemeente Ooststellingwerf (en de door de gemeenteraad ingestelde commissies), de heffingsambtenaar, de invorderingsambtenaar, de leerplichtambtenaar en de ambtenaar van de burgerlijke stand hebben
de heer J.J. Siccama en mevrouw R.M. van der Veen aangesteld als Functionaris Gegevensbescherming (FG).

De FG ziet erop toe dat de AVG intern wordt nageleefd. Het college dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door hem toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en hem de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van zijn deskundigheid.

De gemeente voldoet aan de volgende minimale gestelde 6 AVG-maatregelen:

1. het beschikken over een register van verwerkingsactiviteiten;
2. het kunnen uitvoeren van een data protection impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacyrisico;
3. het beschikken over een register van datalekken die zijn opgetreden;
4. het aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer daarvoor toestemming nodig is;
5. het aangesteld hebben van een Functionaris gegevensbescherming en aangemeld hebben bij de Autoriteit persoonsgegevens;
6. het beschikken over een procedure voor inzage in persoonsgegevens.

De echte gevolgen van de invoering van de AVG gaan echter veel verder dan het voldoen aan de zes verplichte AVG-maatregelen. Om privacy echt goed te borgen zijn goed privacy management en een cultuuromslag nodig, die doordringt in alle lagen van de organisatie, van de baliemedewerker tot de burgemeester en van de procesverantwoordelijke tot de bode.

De Functionarissen Gegevensbescherming hebben voor de komende jaren een controleplan opgesteld waarmee structuur is aangebracht in de werkwijze van de Functionaris Gegevensbescherming. Het controleplan is geschreven om inzicht te geven in de wijze waarop de Functionaris Gegevensbescherming zijn onafhankelijke toezichtrol uitvoert. Dit plan dient ter ondersteuning en vastlegging van de uitvoering van controlewerkzaamheden om aan te kunnen tonen of de gemeente aan de AVG-verplichtingen voldoet en het gemeentelijk privacy- en beveiligingsbeleid naleeft en daarover verantwoording kan afleggen. Het controleplan is in december 2020 ter kennisname gezonden aan directie en college.

Controle AVG
In december 2022 is directie en college geïnformeerd over de uitkomsten van de door de Functionarissen Gegevensbescherming uitgevoerde controle op de algemene borging van de AVG, verder reikend dan de hierboven genoemde minimale eisen waaraan zichtbaar al wordt voldaan. Daar waar vanuit de controle is aangegeven gedeeltelijk criteria te hebben geïmplementeerd (oranje) of zelfs niet te hebben geïmplementeerd (rood), is desondanks de basis op orde, maar wordt **a)** dit niet altijd als zodanig nageleefd, **b)** is dit een gevolg van inrichtingskeuzes of **c)** geen actie ondernomen op basis van risico-inschatting.

Er zijn daarbij geen tekortkomingen geconstateerd op basis waarvan direct actie nodig is. Wel kunnen verbeteringen worden doorgevoerd in de procesgang. De Functionaris Gegevensbescherming vervult hierin een coördinerende rol. De in te zetten acties hebben gezien het risico echter een lage prioriteit.

In mei 2024 is directie en college geïnformeerd over de uitgevoerde hercontrole op de algemene borging van de AVG. Er zijn wederom geen tekortkomingen geconstateerd. Op basis van de hercontrole zijn op een klein aantal punten (ondanks lage risico en lage prioriteit) verbeteringen aangebracht:

1. Het plaatsen van aanvullende informatie op intranet over de uitvoer van een DPIA en verwijzing naar hulpmiddelen en contactpersonen binnen de organisatie met een overzicht welke DPIA's inmiddels hebben plaatsgevonden.

2. Overzicht opgemaakt van de gegevensverwerkingen waarbij gebruik gemaakt wordt van grondslag toestemming (uitzondering).

3. Binnen de afdelingen vraag uitgezet of er nieuwe gegevensverwerkingen zijn sinds de start van de AVG ten behoeve van het actualiseren van de verwerkingsregister.

4. Nieuwe medewerkers worden binnen 3 maanden na indiensttreding geïnstrueerd op informatiebeveiligings – en privacyaspecten als vast onderdeel van het inwerkprogramma binnen HRM via de ontboardingsapp Appical en Olga.

Wpg
De Wpg kent een apart privacy regime. Jaarlijks moet door de werkgever een interne privacy audit worden uitgevoerd en vierjaarlijks een privacy audit door een onafhankelijke gecertificeerde externe auditor.

Het zorgdragen voor de uitvoer van deze audit is een verantwoordelijkheid van de lijn, daar waar betreffende domeinen zijn gehuisvest, evenals het voldoen aan de gestelde normen in het kader van de Wpg. De audit heeft niet alleen betrekking op de opsporingstaken binnen OWO-VTH (voor de 3 gemeenten) maar ook op dergelijke taken binnen onderwijs door de leerplichtambtenaar en in een aantal situaties, indien van toepassing, binnen Werk & Inkomen door de toezichthouder PW.

Binnen de gemeente Ooststellingwerf valt alleen het werkterrein van de leerplichtambtenaar binnen de scope van deze audit..

Onderstaande actiepunten maken onderdeel van het beoordelingskader (opzet en bestaan) van de auditor. Bij tekortkomingen zijn dwingende aanbevelingen van toepassing en is het noodzakelijk een verbeterplan op te stellen.

Actiepunten:

1. Nagaan of de bepalingen voor het verwerken en verstrekken van politiegegevens worden nageleefd.
2. Nagaan of er voldoende onderscheid is tussen het verwerken van persoonsgegevens (toezicht, handhaving, AVG) en het verwerken van politiegegevens (opsporing, Wpg). Bijvoorbeeld door aparte systemen of labelen.
3. Nagaan of er onderscheid is tussen feiten en persoonlijk oordeel.

4. Nagaan of er onderscheid is in categorieën van betrokkenen.
5. Nagaan of de verwerkings- en bewaartermijnen worden nageleefd en de gegevens tijdig worden vernietigd.
6. Nagaan of andere partijen zijn ingeschakeld, zo nodig afsluiten verwerkersovereenkomsten.
7. Nagaan of alle handelingen met politiegegevens worden vastgelegd (logging in geautomatiseerde systemen).
8. Nagaan of er gemeenschappelijke verwerkingen zijn. Zo ja deze melden aan Autoriteit Persoonsgegevens.
9. Bijhouden register van verwerkingen*.
10. Opstellen procedures rechten van betrokkene (informatieplicht, inzage, correctie, vernietigen, afschermen)*.
11. Opstellen procedure meldplicht datalekken*.
12. Opstellen overige noodzakelijke procedures (*nog nader te onderzoeken*).
13. Opstellen privacyverklaring*.
14. Opstellen privacybeleid (gegevensbeschermingsbeleid)*.
15. Documenteren doelen onderzoeken gerichte opsporing (artikel 9-verwerkingen) – *indien van toepassing*.
16. Documenteren verstrekken of doorgifte politiegegevens.
17. Documenteren feitelijke of juridische redenen afwijzen verzoeken van betrokkenen.
18. Documenteren datalekken, inclusief feiten, gevolgen en getroffen maatregelen*.
19. Aanwijzen Bevoegd Functionaris voor artikel 9-verwerkingen (gerichte opsporing) – *indien van toepassing*.
20. Aanwijzen Functionaris Gegevensbescherming voor toezicht op het naleven van de Wpg*
21. Zorgen dat het naleven van de wet- en regelgeving aantoonbaar is*
22. Tenminste jaarlijks een interne audit (laten) uitvoeren op één of meer onderdelen van de Wpg.
23. Iedere vier jaar privacy audit laten uitvoeren en indien nodig binnen 3 maanden een verbeterplan opstellen en binnen 1 jaar een heraudit (laten) uitvoeren.

Allereerst zijn een deel van te nemen acties voor een groot deel vergelijkbaar met acties die eerder in het kader van de AVG zijn (zie * bij de acties) uitgevoerd. Om te voldoen aan deze acties is er zodoende binnen onze gemeente al een basis gelegd. De rol van FG in het kader van de AVG is al binnen onze organisatie onafhankelijk belegd. Bestaande documentatie in het kader van de AVG is van daaruit dusdanig aangepast zodat op deze onderdelen ook wordt voldaan aan de gestelde eisen in het kader van de Wpg.

Controle Wpg
In het 1e kwartaal 2024 hebben de Functionarissen Gegevensbescherming een controle uitgevoerd op de algemene borging van de hierboven genoemde actiepunten en follow up op de dwingende aanbevelingen in het Assurancerapport.

Hieronder volgt een overzicht van acties die inmiddels zijn ondernomen:

1. De directie heeft op advies van de Functionaris Gegevensbescherming in 2022 besloten om ter aanvulling op de AVG, de indiener van dit rapport en Rowena van der Veen ook te benoemen als Functionaris Gegevensbescherming m.b.t. de verwerking van persoonsgegevens in het kader van de Wpg (zie **actiepunt 20 en 21**) en daarvoor gefaseerd stappen te zetten.
2. Op 16 september 2022 heeft de OR ingestemd met het verzoek het gehele privacybeleid te actualiseren en daaraan gekoppeld een wijziging in het Reglement Functionaris voor de Gegevensbescherming door te voeren.
3. Op 29 november 2022 is het geactualiseerde privacy beleid voor interne doeleinden (zie ook 4.1) door het college vastgesteld inclusief Reglement Functionaris voor de Gegevensbescherming (zie **actiepunt 14**). Op 8 maart 2023 is het externe privacybeleid inclusief privacyverklaring door het college vastgesteld (zie **actiepunt 13 en 14**)
4. De indiener van dit rapport en Rowena van der Veen zijn na deze instemming formeel aangewezen als Functionaris Gegevensbescherming voor de Wpg, door het college op 14 maart 2023, bekendgemaakt in het elektronisch gemeenteblad op 18 april 2023 (zie **actiepunt 20 en 21**).
5. Op 8 november 2023 is de geactualiseerde handreiking DPIA inclusief stroomschema vastgesteld door de directie (zie **actiepunt 12**).

6. Op 15 november 2023 is de geactualiseerde procedure rechten van betrokkene vastgesteld door de directie (zie **actiepunt 10**).
7. Op 7 december 2023 is de geactualiseerde procesgang rondom de meldplicht van datalekken vastgesteld door de directie (zie **actiepunt 11 en 18**).
8. Er is specifiek voor de verwerkingen die door de leerplichtambtenaar onder de Wpg plaatsvinden een verwerkingsregister opgemaakt (zie **actiepunt 9**).
9. Partijen die worden ingeschakeld zijn in het verwerkersregister opgenomen, opstellen verwerkersovereenkomsten (geen verwerkersrelatie) daarbij niet van toepassing (zie **actiepunt 6**).
10. De bepalingen voor het verwerken van politiegegevens zijn in de onderzoeksperiode nageleefd (zie **actiepunt 1**).
11. Bij het verwerken van politiegegevens gaat het bij het beoordelen van het relatief of absoluut verzuim in het kader van de Leerplichtwet, uitsluitend om artikel 8 verwerkingen gaat. Artikel 9 verwerking zijn binnen onze gemeente niet van toepassing (zie **artikel 15 en 19**).
12. Externe privacy audit heeft plaatsgevonden in 2022, assurancerapport aangeleverd op 5 december 2022. De herbeoordeling heeft in 2023 binnen gestelde termijn van 1 jaar plaatsgevonden. Het herbeoordelingsrapport is tijdig voor 1 maart 2024 aangeleverd aan de AP. Op advies van de FG is er inmiddels een verbeterrapport opgesteld (norm binnen 3 maanden was hierin niet gerealiseerd) (zie **actiepunt 23**).

Op basis van de uitgevoerde controle blijkt dat actiepunten grotendeels zijn opgepakt. Voor de overige actiepunten is er een verbeterplan opgesteld. De belangrijkste nog te nemen acties;

- Het afschermen van registraties (verwerkingen) in het kader van de Wpg en enkel geautoriseerde personen hierin toegang te verlenen. Binnen de gemeente loopt het project Kernapplicaties (organisatiebreed) waarin dit onderdeel uitmaakt. E.e.a. is nu in de ontwerpfase.
- Overweging om de controle op de juistheid en nauwkeurigheid van de Wpg gegevens te beleggen bij een kwaliteitsfunctionaris (4-ogen principe).

Het college van B&W heeft op 23 april 2024 besloten de BOA-taken in het kader van de Leerplicht met ingang van 1 januari 2025 onder te gaan brengen bij de centrumgemeente Smallingerland..

Tot en met verantwoordingsjaar 2024 dient onze gemeente nog verantwoording af te leggen over verwerkingen in het kader van de Wpg, vanaf verantwoordingsjaar 2025 is dit een taak van de centrumgemeente Smallingerland. De verplicht uit te voeren externe audit door een onafhankelijke gecertificeerde auditor over verantwoordingsjaar 2024 vindt daarmee nog plaats onder onze verantwoordelijkheid, te starten in 2025.

5.1 Meldplicht datalekken

Al sinds 1 januari 2016, maar ook onder de AVG en Wpg, moet de gemeente ernstige datalekken onverwijld (in principe binnen 72 uur) melden aan de Autoriteit Persoonsgegevens en in een aantal gevallen ook aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Er is sprake van een datalek als er als gevolg van een beveiligingsincident kans is op verlies of onrechtmatige verwerking van persoonsgegevens. Het doel van deze meldplicht is het beperken van schade voor de betrokkenen (te weten de personen van wie de gegevens gelekt zijn) en als het mogelijk is het beperken van de omvang daarvan.

Een datalek moet gemeld worden aan de Autoriteit Persoonsgegevens indien er bijzondere persoonsgegevens of gegevens van gevoelige aard zijn gelekt én indien dit leidt tot ernstige nadelige gevolgen voor de persoonlijke levenssfeer van de inwoner ook aan de betrokkenen. Niet melden of nalatigheid kan leiden tot hoge boetes. Door het melden van datalekken bij de Autoriteit Persoonsgegevens kan ook lering getrokken worden uit wat er mis ging om te voorkomen dat nogmaals zo'n datalek plaatsvindt.

De gemeente heeft in 2017 de procedure meldplicht datalekken vastgesteld met daarin een stroomschema voor het melden en afhandelen van een datalek. Deze procedure is in 2019 geactualiseerd in het kader van de AVG en in 2023 geactualiseerd in het kader van de Wpg.

Een aparte situatie doet zich voor in het geval van een datalek waarbij er sprake is van schending van de ambtelijke integriteit, onbevoegd gebruik door een medewerker van systemen waarbij sprake van misbruik en/of fraude. Een vermoeden van een dergelijk strafbaar feit kan ook binnenkomen via de officier van justitie, met tussenkomst van de politie, waarbij wordt verzocht om verstrekking van geraadpleegde gegevens uit systemen. In een dergelijke situatie dient natuurlijk ook de privacy van de desbetreffende medewerker te worden gewaarborgd. Een schending van het ambtsgeheim leidt immers tot ontslag. Het is dan ook van belang het proces op een uniforme wijze te laten verlopen, waarbij alleen een beperkte groep mensen binnen onze organisatie kennis mag nemen van de inhoud. Dit is daarom ter aanvulling op de actualisatie van de procedure meldplicht datalekken in een apart proces vastgelegd en in de vaststelling door de directie meegenomen. Het geheel is laatstelijk vastgesteld op 7 december 2023.

De beveiligingsfunctionaris (CISO) / functionaris gegevensbescherming (FG) is hierbij de contactpersoon richting de Autoriteit Persoonsgegevens en houdt centraal een register bij van de beveiligingsincidenten/datalekken die binnen de gemeente hebben plaatsgevonden.

5.2 Verwerkingsregister en verwerkersovereenkomsten

Burgers hebben met ingang van de inwerkingtreding van de AVG per 25 mei 2018 en in het kader van de Wpg recht op inzage van welke gegevens worden verwerkt, maar ook het recht om gegevens uit de database te verwijderen tenzij legitieme wettelijke vereisten dit voorkomen.

Het in kaart hebben van de wettelijke grondslag van verwerking van persoonsgegevens is in dit kader van groot belang en is opgenomen in het verwerkingsregister. Naast een verwerkingsregister die betrekking heeft op verwerkingen op basis van de AVG, is er een verwerkingsregister opgesteld die betrekking hebben op de Wpg binnen leerplicht. In beide registers is opgenomen welke persoonsgegevens worden verwerkt, wat de grondslag is van deze verwerking en wat het doel is van de verwerking. Voor onze als gemeente is de grondslag meestal gebaseerd op de wettelijke verplichting, publieke taak. Met externe organisaties die in opdracht van onze gemeente persoonsgegevens verwerkt dient een verwerkersovereenkomst te worden gesloten. Hiervoor hanteren we als leidraad de standaard verwerkersovereenkomst die beschikbaar is gesteld door de Informatiebeveiligingsdienst (IBD) welke voldoet aan de landelijke normen.

5.3 Data protection impact assessment

Onder de Algemene verordening gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) kunnen organisaties verplicht zijn een data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

Verplichte DPIA
In de AVG, Wpg en Wjsg is op hoofdlijnen aangegeven wanneer een DPIA verplicht is. Dat is het geval als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Dit moet de gemeente als verwerkingsverantwoordelijke zelf bepalen waarbij als hulpmiddel gebruik kan worden gemaakt van criteria welke zijn opgesteld door de Autoriteit Persoonsgegevens. Indien er sprake is van een gegevensverwerking met een hoog privacyrisico dan mag niet eerder met het verwerken van gegevens worden gestart voordat een DPIA (en indien nodig een voorafgaande raadpleging bij de AP) is uitgevoerd. Het uitvoeren van een DPIA is een lijnverantwoordelijkheid. Bij het uitvoeren van een DPIA moet advies worden ingewonnen bij de Functionaris voor de gegevensbescherming (FG). Dit geeft extra zekerheid dat de DPIA voldoende zicht geeft op de risico's en er voldoende maatregelen worden getroffen om deze af te dekken. Uiteraard is het eerst van belang te bepalen of de voorgestelde gegevensverwerking rechtmatig is. Daarnaast heeft de Autoriteit Persoonsgegevens een lijst opgesteld van bestaande gegevensverwerkingen waarbij het ook noodzakelijk is een DPIA uit te voeren. De Functionarissen

Gegevensbescherming hebben een handreiking opgesteld met daarbij een stroomschema, laatstelijk vastgesteld door de directie op 8 november 2023, als hulpmiddel binnen de vakafdelingen om te kunnen bepalen of er al dan niet een DPIA noodzakelijk is.

Gegevensverwerkingen waarbij vastgesteld dat de uitvoer van een DPIA noodzakelijk is:

1. Wet verplichte geestelijke gezondheidszorg (Wvggz)

Per 1 januari 2020 is de Wet verplichte geestelijke gezondheidszorg (Wvggz) in werking getreden. De Wvggz is de opvolger van de BOPZ (Wet bijzondere opneming psychiatrische ziekenhuizen). De Wvggz definieert een aantal taken voor (onder anderen) de gemeenten. Om die taken uit te kunnen voeren moet de gemeente persoonsgegevens verwerken. Daarnaast is het op grond van de wet, en voor de juiste uitvoering daarvan, noodzakelijk dat de gemeente persoonsgegevens deelt met andere partijen (o.a. GGZ, politie, Openbaar Ministerie) en met betrokkene zelf, of zijn vertegenwoordiger(s). In de uitvoering van de Wvggz worden gevoelige persoonsgegevens én bijzondere persoonsgegevens verwerkt van personen in een kwetsbare positie.

De Wvggz heeft in het kort vier doelen:
1. Het versterken van de rechtspositie van personen met een psychische stoornis aan wie tegen hun wil zorg wordt verleend;
2. De noodzaak van dwang en de duur ervan te beperken.
3. Het verhogen van de kwaliteit van verplichte zorg door het bieden van zorg op maat waarbij randvoorwaarden moeten worden gecreëerd om mensen met een psychische stoornis weer succesvol deel te laten nemen aan het maatschappelijk leven;
4. Een betere rolverdeling tussen de verschillende actoren die betrokken zijn bij gedwongen zorg.

Met de invoering van de Wvggz krijgt de gemeente een aantal nieuwe taken toebedeeld en worden bestaande taken gewijzigd. De drie belangrijke onderdelen in de wet waar de gemeenten een rol hebben zijn de crisismaatregel, de zorgmachtiging en het periodiek overleg.

Friese gemeenten hebben besloten genoemde taken onder te brengen bij GGD Fryslân, vastgelegd in een dienstverleningsovereenkomst.

Vanuit de VNG is in december 2019 de uitgevoerde DPIA, in de vorm van een algemene effectbeoordeling, opgeleverd op de uitvoering van de Wvggz. Met deze algemene effectbeoordeling is een specifieke DPIA door elke individuele gemeente niet meer noodzakelijk. Onze gemeente kan hiernaar verwijzen. De uitgevoerde DPIA is gereviewd door:
- een werkgroep van gemeenten (circa 20 gemeentelijke medewerkers: Wvggz deskundigen, FG's van gemeenten en privacy deskundigen van gemeenten)
- de IBD-gemeenten
- een onafhankelijk privacyjurist
- De FG van de firma Khonraad

De DPIA is – conform de bedoeling van de AVG – een levend document. In 2024 tot nu hebben hierin geen wijzigingen plaatsgevonden.

2. Aanpak ondermijning

Er wordt van gemeenten veel verwacht in de aanpak van georganiseerde ondermijnende criminaliteit onder meer binnen het kader van de RIEC-samenwerking alsmede in het kader van de eigen taakuitvoering. Voor een effectieve aanpak van deze ondermijnende activiteiten (en mogelijk georganiseerde criminaliteit) is een geintegreerde bestuurlijke aanpak binnen de gemeente een noodzakelijk vereiste. De signalen, afkomstig van burgers en organisaties, dienen als input voor het signaleren van ondermijnende en mogelijk georganiseerde criminaliteit. Bij de aanpak van ondermijning geldt dat er mogelijk bijzondere persoonsgegevens en strafrechtelijke gegevens worden verwerkt.

In 2019 zijn er inmiddels acties ondernomen om te komen tot een plan van aanpak. De FG's van de gemeente Ooststellingwerf hebben daarom geadviseerd dat de uitvoer van een DPIA noodzakelijk is

en daarnaast een privacy protocol op te stellen om te voldoen aan de privacywetgeving. Bij de uitvoering kan als basis gebruik gemaakt worden van reeds uitgevoerde DPIA's door andere gemeenten, waaronder Groningen en Leeuwarden.

In 2021 is er een start gemaakt om het proces rond ondermijning binnen de gemeente in te richten. Zo is er inmiddels een meldpunt, waar collega's meldingen kunnen doen van mogelijke ondermijning. Zodra de processen zijn beschreven kunnen de risico's middels een DPIA in kaart worden gebracht.

Op basis van de DPIA's van andere gemeenten is de conclusie dat er een grondslag is voor het verwerken van persoonsgegevens voor activiteiten in het kader van ondermijning als geheel en daarmee sprake van een rechtmatige verwerking. Dit geldt ook ten aanzien van het eventuele gebruik van de brache- en bibobscan, beschikbare tooling bij de aanpak van ondermijning. Het is hierin zaak blijvend de risico's in kaart te brengen en passende technische en organisatorische beveiligingsmaatregelen te treffen. Op 30 oktober 2023 is het eindadvies van de FG opgeleverd en opgenomen in de uitgevoerde DPIA 2023. Het geheel is met advies voorgelegd aan het college van B&W. Het Privacy Protocol bestuurlijke aanpak ondermijning Ooststellingwerf is door het college vastgesteld op 14 november 2023. Jaarlijks zal het proces worden geëvalueerd met ruimte voor wijzigingen en worden getoetst aan de eisen van de AVG.

3. Zaakgericht werken

In februari 2020 is het college middels een memo geïnformeerd over het zaakgericht werken in relatie tot de privacywetgeving. Aanleiding was een klacht van een buiten gemeentelijke inwoner waarbij uit nader onderzoek is gebleken dat er meer persoonsgegevens zijn vastgelegd dan noodzakelijk en daarmee de huidige werkwijze van het zaakgericht niet voldoet aan de wet BRP en de privacywetgeving. Op advies van de Functionarissen Gegevensbescherming van de OWO-gemeenten is er een DPIA (Data Protection Impact Assessment) uitgevoerd door een extern bureau. De reikwijdte betrof de keten van zaakgericht werken.

Belangrijke conclusie is dat DIV met de huidige werkwijze de GBA-V wel mag raadplegen voor het inboeken van post in het zaaksysteem wanneer het gaat om de wettelijke taken zoals vastgelegd in het autorisatiebesluit. Het autorisatiebesluit gaat daarbij uit van een wettelijke taak. Een algemene, niet (altijd) op de wet gebaseerde taak voor het inboeken van alle post, zoals het afhandelen van informatieverzoeken en dergelijke, valt hier echter niet onder.

In 2021 is besloten het proces voor het inboeken van overige post van buitengemeentelijke personen dusdanig aan te passen dat hiermee aan de Wet Brp en de AVG wordt voldaan.

Op basis van de uitgevoerde DPIA heeft de Functionaris Gegevensbescherming een eindadvies opgesteld en daarin aanbevelingen gedaan op de bevindingen. In het college van 17 mei 2022 is besloten de aanbevelingen op te volgen, welke inmiddels zijn geïmplementeerd, hieronder weergegeven:

Bevinding 1
Verantwoordelijkheden rondom (toezicht op) de gegevensverwerking zijn beperkt en niet formeel vastgelegd. In de OWO-samenwerking blijft iedere partij afzonderlijk verantwoordelijk voor de gegevensverwerking van de eigen gemeente. In de OWO-samenwerking is (informeel) afgesproken dat Weststellingwerf leidend is bij het beschermen van persoonsgegevens binnen DIV. Daarnaast zal de Functionaris Gegevensbescherming van Weststellingwerf toezicht houden op deze gegevensverwerking door DIV binnen de OWO-samenwerking. De drie gemeenten blijven te allen tijde zelf verantwoordelijk voor de gegevens die binnen hun eigen omgeving - al dan niet door de OWO-samenwerking – worden verwerkt.

Aanbeveling FG
Uitbreiden van de regeling gezamenlijke verantwoordelijkheid OWO of instemmen met de onderlinge werkafspraken van de FG's/CISO's en wie (welke gemeente, CISO,FG) wanneer aanspreekpunt is voor de AP.

Opvolging
De counterparts OWO hebben de onderlinge werkafspraken besproken en voor kennisgeving aangenomen.

Bevinding 2
Neem in de privacyverklaring van alle drie de gemeenten informatie op over de OWO-samenwerking(en eventuele andere gemeentelijke samenwerkingen) en de taken die binnen deze samenwerking vallen. Licht hierin (kort) toe hoe de gegevens worden verwerkt en voor welk doel.

Aanbeveling FG
Ons advies is het privacybeleid op de website van de Gemeente Ooststellingwerf uit te breiden met de OWO-samenwerking.

Opvolging
Het privacybeleid en de privacyverklaring is geactualiseerd en vastgesteld door het college op 7 maart 2023. Hierin wordt verwezen naar de OWO-samenwerking en de gegevensuitwisseling tussen de gemeenten onderling.

4. MDA++

In 2020 is de pilot Multi Disciplinaire Aanpak++ Lokaal (MDA++ Lokaal) gestart die in OWO verband wordt opgepakt. In deze pilot worden gezinnen waar er sprake is van meervoudige problematiek en structurele onveiligheid voor langere tijd gemonitord door een lokaal MDA team volgens de MDA++ methodiek. In opdracht van de OWO-gemeenten heeft een externe partij in 2021 de opdracht gekregen om volgens de regels van de privacywetgeving (de AVG) te beschrijven en te beoordelen in welke mate MDA++ LOKAAL en de daarmee gemoeide gegevensverwerkingen voldoen aan de vereisten van de AVG.

In de rapportage ‘Data Protection Impact Assessment MDA++ Lokaal’ zijn de belangrijkste risico’s geïdentificeerd en zijn er maatregelen voorgesteld ter verbetering. Deze maatregelen zijn vervolgens uitgewerkt in het ‘plan van aanpak DPIA’ en voorgelegd aan de FG’s binnen OWO voor een eindadvies.

Belangrijkste bevinding:
De AVG vereist dat bij de verwerking de vertrouwelijkheid en integriteit en daarmee ook de beschikbaarheid van de persoonsgegevens van betrokkenen wordt gewaarborgd. Dit geldt ook voor het systeem waar dossiers in worden opgeslagen. Het cliëntvolgsysteem ‘Samen1plan’ voldoet hier niet aan.

Naar aanleiding van de beveiligingsrisico’s heeft de afdeling daarom besloten per direct te stoppen met “Samen1plan”. In plaats daarvan is gebruik gemaakt van een tijdelijke interne IT – oplossing bij de gemeente (intranet) die aan de voorwaarden conform de AVG voldoet. Bij een hernieuwde voortzetting moet dit alternatief eerst weer worden getoetst op eventuele risico’s en worden voorgelegd aan de Functionarissen Gegevensbescherming.

5. Vroegsignalering schulden

Het doel van vroegsignalering is het eerder in beeld krijgen van cliënten met (beginnende) financiële problemen om daarmee in gesprek te komen, de reguliere betalingen te hervatten en een oplossingsrichting te geven voor de ontstane problemen.

Besluit de gemeente tot het uitvoeren van vroegsignalering, dan moet zij dit expliciet als taak ter uitvoering van de Wgs in het gemeentelijk plan opnemen. Het benoemen van vroegsignalering als gemeentelijke taak en vervolgens het doel dat de gemeente met die taak wil bereiken is de basis voor het proces vroegsignalering en de daarbij behorende gegevensverwerking. Met het oog op een zorgvuldige gegevensverwerking sluit de gemeente aan bij de landelijke convenant, zijn er aanvullende overeenkomsten opgesteld, en is het proces nader uitgewerkt waarmee duidelijk de actoren, juridische positie en afspraken zijn vastgelegd. Daarnaast sluit de gemeente als

opdrachtgever een verwerkersovereenkomst met BKR. Met de DPIA zijn, ter aanvulling op de landelijke DPIA vanuit de VNG, binnen de afdeling de privacy risico's in kaart gebracht en afgedekt. In het werkplan is een eerste aanzet gegeven aan de in te zetten interventies en prioritering. Dit zal jaarlijks worden geëvalueerd en mogelijk kunnen leiden tot aanpassingen.

Met de reeds getroffen en voorgenomen acties voldoet de gegevensverwerking aan de gestelde eisen in het kader van de AVG. Er zijn daarmee geen belemmeringen om in te zetten op vroegsignalering. Het verdient aanbeveling om periodiek het proces te evalueren om van daaruit vast te kunnen stellen, in verband met eventuele wijzigingen, dat privacy risico's nog steeds worden afgedekt.

6. Cameratoezicht

Als gevolg van de invoering van de AVG zijn we als organisatie wettelijk verplicht een zogenaamde privacy impact analyse uit te voeren als onze organisatie ondermeer op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied, bijvoorbeeld via cameratoezicht. Deze DPIA is uitgevoerd op het cameratoezicht in en om gemeentelijke gebouwen en gebouwen die in eigendom van de gemeente zijn in samenwerking met Team Dienstverlening en de privacy-functionaris (binnen BJZ).

Dit cameratoezicht heeft tot doel de veiligheid van medewerkers en bezoekers te vergroten en eigendommen te bewaken. De camera's hebben zowel een preventief (afschrikeffect) als repressief (ondersteuning bij opsporing naar aanleiding van calamiteiten of ongewenst/crimineel gedrag) doel. Incidenten als diefstal, beschadiging van eigendommen, overval, fraude, ongewenst en agressief gedrag worden met het cameratoezicht tegengegaan en geregistreerd.

Op basis van de uitgevoerde DPIA zijn er een aantal bevindingen op basis waarvan stappen worden ondernomen om de risico's te beperken. In 2022 is ook de camera bij de Bosbergtoren hierin toegevoegd. Het eindadvies van de FG is op 29 april 2024 opgesteld. Belangrijkste constatering is dat er sprake is van een rechtmatige verwerking in het kader van de AVG maar op dit moment nog geen cameraprotocol of –beleid is opgesteld. Hierdoor ontbreken specifieke normen voor het gebruik van de camera's zoals over de wijze van toepassing, informatieverstrekking, toegang tot apparatuur en opnames, opslag en bewaartermijnen. De nog te treffen maatregelen zijn opgenomen in een monitoringsoverzicht. De FG houdt toezicht op de voortgang van deze actiepunten, e.e.a. loopt door in 2025.

7. Flexwhere

Als gevolg van het hybride werken maken we binnen onze gemeente gebruik van flexwhere als reserveringssysteem. Medewerkers werken wisselend thuis en op locatie. Daarnaast wordt binnen het gemeentehuis gewerkt met 'flexplekken'. De werkgever wil hiermee bereiken dat medewerkers kunnen zien wie op kantoor zijn en wie extern werken. Ook vanuit het oogpunt bij calamiteiten inzichtelijk te hebben wie in het gemeentehuis aanwezig is, denk hierbij aan ontruimingen. Bij gebruik van een dergelijk systeem is het mogelijk eigen medewerkers te kunnen volgen ook al is het daarvoor niet bedoeld. Het is daarom noodzakelijk dat de privacy van onze medewerkers is geborgd en de privacyrisico's inzichtelijk te maken.

De applicatie biedt voldoende waarborgen voor de bescherming van persoonsgegevens en biedt tevens voldoende maatregelen een inbreuk op de persoonsgegevens te minimaliseren. Er is een verwerkersovereenkomst gesloten. De restrisico's zijn daarmee acceptabel. Er is sprake van een rechtmatige gegevensverwerking in de zin van de AVG.

In het eindadvies van de FG op 29 april 2024 is aangegeven te steunen op de DPIA waarin is aangegeven dat instemming van de Ondernemingsraad vereist is bij een personeelsvolgsysteem. Vanuit HRM is echter voldoende beargumenteerd dat er bij het gebruik van Flexwhere geen sprake is van een personeelsvolgsysteem in de zin van de WOR. Het eerder opgemaakte eindadvies is hiermee op 6 mei 2024 gecorrigeerd.

8. Voorzieningenwijzer

Vanuit de Wet gemeentelijke schuldhulpverlening (Wgs) bieden we inwoners hulp bij het oplossen van financiële problemen en schulden. We helpen inwoners bij het oplossen van financiële problemen en ondersteunen inwoners met het vergroten van de financiële zelfredzaamheid. Onze hulp bieden we zo vroeg mogelijk aan, zodat problematische schulden zoveel mogelijk worden voorkomen. Met ingang van 1 januari 2021 is de Wgs gewijzigd. Deze wetswijziging faciliteert de uitwisseling van persoonsgegevens bij een tweetal onderdelen:

a) de gegevensuitwisseling met als doel vroegsignalering van schulden;
b) de gegevensuitwisseling voor het besluit over toegang tot en het plan van aanpak voor schuldhulpverlening.

Als onderdeel van de Wgs is eerder een DPIA uitgevoerd op het proces van vroegsignalering, waarin door de Functionarissen Gegevensbescherming al een positief eindadvies is opgenomen (zie onder 5, pagina 19).

Gemeenten hebben te maken met een toenemende problematiek rond armoede en problematische schulden. Woningcorporaties ervaren steeds meer problemen met de betaalbaarheid van hun woningen. Om hierin te kunnen voorzien is het instrument De VoorzieningenWijzer opgericht. De VoorzieningenWijzer helpt mensen met inkomens tot modaal bij het kiezen en aanvragen van allerlei voorzieningen die in belangrijke mate de koopkracht kunnen verbeteren. Daarmee verminderen de risico's van huurachterstanden, armoede en problematische schulden.

De VoorzieningenWijzer is een belangrijke oplossing binnen de Nederlandse Schuldhulproute (NSR), waarop wij als gemeente zijn aangesloten. De Nederlandse Schuldhulproute (NSR) en de VoorzieningenWijzer werken samen om de onzichtbare groep mensen met geld- en schuldzorgen in een vroeg stadium te bereiken en te helpen.

Toestemming
De voornaamste grondslag voor de verwerking van persoonsgegevens is de ondubbelzinnig en vrijelijk verkregen toestemming van betrokkene. De intake voor het invullen van de VoorzieningenWijzer vindt plaats als gevolg van natuurlijke contactmomenten in het kader van uiteenlopende gemeentelijke taken. Uiteraard alleen dan wanneer de bevindingen uit die contactmomenten daartoe aanleiding geven. Op geen enkele wijze heeft de keuze om de VoorzieningenWijzer in te vullen voor betrokkene negatieve, maar evenmin positieve, gevolgen als het gaat om zijn relatie met de gemeente of de hem al dan niet toekomende rechten of voorzieningen.

Op 5 september 2023 heeft het college kennis genomen van het eindadvies op de uitgevoerde DPIA van de FG. Met de reeds getroffen en voorgenomen acties voldoet de gegevensverwerking aan de gestelde eisen in het kader van de AVG. Verder zijn er, rekening houdende met de voorgenomen acties, geen belemmeringen om in te zetten op het gebruik van de VoorzieningenWijzer. Het verdient aanbeveling om periodiek het proces te evalueren om van daaruit vast te kunnen stellen, in verband met eventuele wijzigingen, dat privacyrisico's nog steeds worden afgedekt.

9. Informatieknooppunt Zorgfraude

Onze gemeente was in 2023 voornemens om aan te sluiten op het Informatieknooppunt Zorgfraude (IKZ). Het Informatieknooppunt Zorgfraude (IKZ) helpt gemeenten door het verrijken van signalen van een vermoeden van fraude in het zorgdomein. Op deze manier is de gemeente in staat om krachtiger op te kunnen treden tegen malafide zorgaanbieders. Bij het signaleren en aanpakken van zorgfraude vindt er een uitwisseling van gegevens plaats tussen onder andere de gemeente en het IKZ.

Ook organisaties als de Belastingdienst, de Nederlandse Arbeidsinspectie en het OM werken samen in het IKZ. De gegevens kunnen zowel persoonsgegevens als gegevens over bedrijven en andere organisaties zijn. De gemeente zou met hulp van het IKZ een verdiepend onderzoek uitvoeren en op basis daarvan zo nodig actie te ondernemen.

De VNG is tijdelijk gestopt met het delen van persoonsgegevens in het Informatie Knooppunt Zorgfraude (IKZ). De Autoriteit Persoonsgegevens had eerder geen bezwaar tegen deze gegevensdeling. Na intern onderzoek concludeert de VNG echter dat er op dit moment geen robuuste grondslag is om persoonsgegevens te delen, daarmee onrechtmatig in de zin van de AVG.

Onze gemeente is daarom ook niet aangesloten bij het IKZ. Per 1 januari 2025 is de Wet bevorderen samenwerking en rechtmatige zorg gedeeltelijk in werking. Onder deze wet wordt het IKZ een stichting met een wettelijk taak en is onze gemeente bij wet aangesloten.

Weliswaar is er in het kader van deze aanstaande wet dan een grondslag, wel is het noodzakelijk een DPIA op de gegevensverwerking uit te voeren.

10. Gebruik elektrische deelauto Duorsum

In Nederland is in 2019 het Klimaatakkoord afgesloten. Daarin hebben overheden, werkgevers en maatschappelijke organisaties afspraken gemaakt om de CO2-uitstoot te verminderen. Een van de afspraken is dat werkgevers met 100 of meer werknemers hun jaarlijkse CO2-uitstoot door werkgebonden personenmobiliteit verminderen. Gemeente Ooststellingwerf wil deze doelstelling bereiken door de inzet van deelauto's van Duorsum, in samenwerking met Auto Kort.

Het 'Besluit CO2-reductie werkgebonden personenmobiliteit', inwerkingtreding per 1 juli 2024, verplicht werkgevers jaarlijks gegevens over werkgebonden personenmobiliteit te verstrekken.

Het gaat om alle zakelijke ritten en het woon-werkverkeer van werknemers in Nederland, al zijn er uitzonderingen van toepassing. In principe gaat het om reizen waarvoor werknemers een financiële vergoeding ontvangen of waarvoor een voertuig of vervoersbewijs aan werknemers ter beschikking worden gesteld. Rapportage vindt plaats over de jaartotalen van het aantal kilometers, het gebruikte vervoermiddel en het soort brandstof. Dergelijke gegevens mogen niet herleidbaar zijn naar personen. Bij de aanlevering van gegevens voor de rapportageverplichting wordt rekening gehouden met de privacy van werknemers.

WeGo-carsharing wordt ingezet om duurzame dienstreizen mogelijk te maken voor de medewerkers van de gemeente Ooststellingwerf. Medewerkers kunnen via een gebruikersaccount in de WeGo-app een auto reserveren. Medewerkers kunnen ook een dienstreis maken met de deelfiets, openbaar vervoer of eigen vervoer. WeGo-carsharing verwerkt locatiegegevens waardoor gegevens gebruikt kunnen worden om medewerkers te volgen of te monitoren. Het is daarom noodzakelijk dat de privacy van onze medewerkers is geborgd en de privacyrisico's inzichtelijk te maken. Daarnaast is ook instemming van de OR vereist.

Op 22 april 2024 heeft de FG het eindadvies uitgebracht. Er is sprake van een rechtmatige verwerking in de zin van de AVG. Met de app kunnen medewerkers worden gevolgd, tracking. Het instemmingsbesluit van de OR d.d. 4 april 2024 geeft als belangrijkste maatregel voldoende basis om het project te starten.

De gegevens die volgens de rapportageverplichting moeten worden verstrekt, zijn waarschijnlijk niet meteen volledig beschikbaar. Sommige gegevens zijn al aanwezig in onze administratie binnen Youforce, andere gegevens zijn daaraan nog toe te voegen zoals bij het gebruik van de deelauto's via de WeGo-app. Vooruitlopend op de inwerkingtreding per 1 juli 2024 is het daarom noodzakelijk zo snel mogelijk te gaan starten.

Er zijn voldoende maatregelen getroffen om de risico's voor onze medewerkers te beperken. Over de voortgang van de actiepunten is het noodzakelijk de FG te informeren.

11. Overige:

Inburgering, Montr app ten behoeve van huisbezoek in het kader van toezicht, Track & Trace, Informatieknooppunt Zorgfraude (IKZ).

De Functionaris Gegevensbescherming heeft gewezen op het moeten uitvoeren van een DPIA in het kader van gegevensverwerkingen, zoals hierbij opgesomd. Op dit moment is er nog geen volledig beeld van de procesgang. E.e.a. loopt door in 2025.

5.4 Rechten van betrokkenen

De gemeente dient degene waar de gegevens van verwerkt worden (de betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen genomen worden om onrechtmatige toegang en verwerking te voorkomen. Daartoe beschikt de gemeente over een verwerkingsregister (**zie 5.2**). Daarnaast stelt de AVG en Wpg betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens. De rechten van betrokkene maken onderdeel uit van het privacybeleid en de privacyverklaring welke is gepubliceerd op onze gemeente website. Hoe intern om te gaan wanneer een betrokkene een beroep doet op zijn of haar rechten, is vastgelegd in een procedure, geactualiseerde versie laatstelijk vastgesteld door de directie op 15 november 2023. Daarin is ook de rol van de privacy functionaris opgenomen, verantwoordelijk voor de afhandeling van inzageverzoeken en meer uitvoerende privacyvraagstukken.

In verband met de te hanteren functiescheiding kan deze taak niet door de Functionarissen Gegevensbescherming worden uitgevoerd. De rol van privacy functionaris is onafhankelijk buiten de lijn onder bedrijfsvoering belegd. De privacy functionaris informeert de Functionaris Gegevensbescherming. Op deze wijze is de vereiste functiescheiding geborgd.

Hieronder per jaar een overzicht van het aantal binnengekomen verzoeken, welke zijn afgehandeld sinds de invoering van de AVG:

2019:
2 verzoeken om inzage in het dossier
1 correctieverzoek
1 verzoek om informatie
1 klacht waarbij is aangegeven dat onze gemeente teveel gegevens verwerkt*.

*Deze klager heeft zich tevens gewend tot de Autoriteit Persoonsgegevens waarna de Autoriteit Persoonsgegevens contact heeft opgenomen met de FG's van de gemeente Ooststellingwerf. Uit onderzoek is gebleken dat bij het inboeken van post, taak DIV in Weststellingwerf, in het geautomatiseerde proces meer gegevens worden vastgelegd dan noodzakelijk. Dit is kortgesloten met de leverancier PINK en aangepast. De medewerkers van DIV zelf hebben niet meer gegevens geraadpleegd dan alleen naam, adres en woonplaats. De klacht van betrokkene is terecht, de gegevensverwerking was ongewenst en onrechtmatig. De FG van de gemeente Ooststellingwerf heeft betrokkene per brief geïnformeerd en een kopie gezonden aan de Autoriteit Persoonsgegevens.

2020:
4 algemene inzageverzoeken* (waarvan 2 buiten behandeling gesteld).

*Bij een algemene inzageverzoek wordt door de burger gebruik gemaakt van het recht te willen weten welke persoonsgegevens de gemeente verwerkt, waarvoor we deze gegevens precies gebruiken en met wie deze eventueel worden gedeeld. Betrokkene kan alleen gegevens van zichzelf opvragen en moet zich kunnen legitimeren. Bij gegevens van een kind jonger dan 16 jaar doet een ouder of wettelijk vertegenwoordiger het inzageverzoek. Hij/zij moet zich dan ook legitimeren. Als de indiener zich niet wil of kan identificeren is dit grond om het verzoek af te wijzen.

De afhandeling van een algemene inzageverzoek wordt verricht door de privacyfunctionaris binnen het bestuurlijk juridisch cluster en binnen de gehele organisatie uitgezet.

2021:
1 inzageverzoek (dossierinhoudelijk)
2 verzoeken om verwijdering van gegevens.

Een inzageverzoek in het dossier wordt afgehandeld door de betreffende vakafdeling, in dit geval binnen het sociale domein.

Betrokkene heeft onder bepaalde voorwaarden het recht om ‘vergeten’ te worden. Dit betekent dat de gemeente zijn/haar gegevens verwijdert. Dit kan wanneer:
- de persoonsgegevens niet langer noodzakelijk zijn voor het doel waarvoor de gegevens verzameld zijn en er geen andere reden is om deze persoonsgegevens te bewaren;
- het doel voor het verwerken van de persoonsgegevens is gebaseerd op de toestemming betrokkene en hij/zij die toestemming intrekt;
- betrokkene bezwaar heeft gemaakt tegen de verwerking en de gemeente geen zwaarwegende gronden heeft om de gegevens te verwerken;
- de persoonsgegevens onwettig zijn verwerkt;
- de persoonsgegevens moeten worden gewist om te voldoen aan Europese of Nederlandse wetgeving.

Eén verzoek om verwijderding is buiten behandeling gesteld. Bij het andere verzoek is gebleken dat slechts een gedeelte van de gegevens nog langer bewaard mocht worden. In dit geval zijn de overige gegevens verwijderd.

2022:
3 verzoeken om verwijdering van gegevens, waarvan 1 buiten behandeling gesteld.

2023:
2 inzageverzoeken, waarvan 1 buiten behandeling gesteld.
2 verwijderverzoeken, waarvan 1 buiten behandeling gesteld.

2024:
1 inzageverzoek.

6 Dreigingen, risico’s en trends

Naast de risico’s voor informatieveiligheid en privacy die de gemeente zelf in kaart brengt, zijn er landelijke en wereldwijde dreigingen. Jaarlijks brengt het NCSC het Cybersecuritybeeld Nederland uit. Hierin staan de dreigingen en trends vermeld waar Nederland mee te maken heeft of krijgt, te weten cryptoware, ransomware, phishing, inbreuken op de digitale veiligheid door geopolitieke spanningen, kwetsbaarheden in software en inbreuken op beschikbaarheid van informatiesystemen. Gemeenten moeten weerbaar zijn tegen dit soort dreigingen om de dienstverlening en bedrijfsvoering voort te kunnen zetten. Aangezien cybercriminaliteit zich meestal niet beperkt tot stadsgrenzen of landelijke grenzen, zijn deze dreigingen in meer of mindere mate ook voor gemeenten van toepassing. De gemeente is aangesloten bij de Informatiebeveiligingsdienst (IBD).

Vanuit de IBD worden gemeenten op de hoogte gesteld van ernstig kwetsbaarheidsrisico’s in software waarin bij misbruik, verstoring of uitval dit gevolgen kan hebben voor de gemeentelijke dienstverlening. Op basis van dergelijke meldingen vindt er binnen I&A vervolgens een risico/impactanalyse plaats om de risico’s te mitigeren.

De Informatie Beveiligingsdienst (IBD) is een gezamenlijk initiatief van de VNG en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De IBD is opgericht vanwege het grote aantal incidenten op informatiebeveiligingsvlak. Het IBD geeft concrete ondersteuning om gemeenten te helpen informatiebeveiliging naar een hoger plan te tillen.
Aansluiting betekent enerzijds dat de gemeente een aantal zaken dient in te richten om de IBD dienstverlening af te nemen en anderzijds dat de ICT-verantwoordelijke over concrete informatie moet kunnen beschikken om gericht te kunnen handelen.

De ondersteuning van het IBD richt zich op een drietal punten:

1. Incidentpreventie, bestaande uit kwetsbaarheidswaarschuwingen teneinde incidenten te voorkomen;
2. Incidentdetectie, bestaande uit het waarschuwen van gemeenten waarvan bekend is dat ze geïnfecteerde systemen hebben;
3. Incidentcoördinatie, bestaande uit het beperken van de technische-, financiële- en imagoschade indien zich incidenten voordoen.

Jaarlijks publiceert de IBD het Dreigingsbeeld voor Nederlandse gemeenten. Het dreigingsbeeld is geschreven voor het management. De inhoud van het dreigingsbeeld wordt indien nodig door de beveiligingsfunctionaris (CISO) omgezet in een actieplan.

7 Audits, kwetsbaarheidstesten en steekproeven

In 2024 zijn in het kader van verplichtende zelfregulering meerdere zelfevaluaties uitgevoerd, te weten voor de basisregistratie personen (BRP) en voor de waardedocumenten (PNIK). De vragen m.b.t. de BRP en PNIK in de ENSIA tool zijn vooral HRM en ICT-gerelateerd; de uitvoer van de inhoudelijke zelfevaluatie m.b.t. BRP en PNIK dient nog steeds plaats te vinden in de Kwaliteitsmonitor. De zelfevaluaties worden in de Kwaliteitsmonitor uitgevoerd door de beveiligingsbeheerder BRP. De beveiligingsfunctionaris (CISO) is daarbij aanwezig om de onafhankelijkheid te waarborgen.

De antwoorden uit de ENSIA-tool worden in een aparte rapportage verwerkt en binnen het Team Dienstverlening verder verwerkt voor upload in de Kwaliteitsmonitor.

De uitkomsten van deze zelfevaluaties zijn gestuurd naar de betreffende toezichthouder, te weten de Rijksdienst voor Identiteitsgegevens (RvIG), het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de Autoriteit Persoonsgegevens.

Zelfevaluatie BRP

Op grond van de wet basisregistratie personen (BRP) is iedere Nederlandse gemeente verplicht om jaarlijks een onderzoek uit te voeren naar de inrichting, de werking en de beveiliging van de basisregistratie, alsmede naar de verwerking van gegevens in de basisregistratie, voor zover het de gemeentelijke voorziening betreft of het college verantwoordelijk is voor de bijhouding.

In de gemeente Ooststellingwerf wordt dit onderzoek uitgevoerd door de beveiligingsbeheerder BRP in bijzijn van de beveiligingsfunctionaris (CISO) die hiervoor door B&W is benoemd. Daarnaast heeft het agentschap BPR een bestandscontrole uitgevoerd.

Voor het onderzoek en de bijbehorende rapportage aan de minister wordt gebruik gemaakt van de Kwaliteitsmonitor, een door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties beschikbaar gestelde online toepassing. De Kwaliteitsmonitor geeft zowel per categorie als voor het gehele proces een objectief oordeel over de kwaliteit.

Uit de uitgevoerde zelfevaluatie blijkt, dat de gemeente Ooststellingwerf met een totaalscore van **94,3%** (vorig jaar 98,8%) vanuit de Kwaliteitsmonitor en een totaalscore van **97%** (vorig jaar 97%) vanuit ENSIA, voldoende scoort op de inrichting, de werking en de beveiliging van de basisregistratie Personen. De gemeente Ooststellingwerf voldoet daarmee aan de wettelijke norm van **90%**.

Zelfevaluatie PNIK (waardedocumenten)

Op grond van de Paspoortuitvoeringsregeling Nederland (PUN) is iedere Nederlandse gemeente verplicht om jaarlijks in de vorm van een zelfevaluatie onderzoek uit te voeren naar de kwaliteit en veiligheid van het aanvraag- en uitgifteproces Paspoorten en Nederlandse Identiteitskaarten. In de gemeente Ooststellingwerf worden deze zelfevaluatie en verdere kwaliteitscontroles uitgevoerd door de beveiligingsbeheerder BRP in bijzijn van de beveiligingsfunctionaris (CISO) die hiervoor door B&W is benoemd.

Voor het onderzoek en de bijbehorende rapportage aan de minister wordt gebruik gemaakt van de Kwaliteitsmonitor, een door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties beschikbaar gestelde online toepassing. De Kwaliteitsmonitor geeft zowel per categorie als voor het gehele proces een objectief oordeel over de kwaliteit. De resultaten dienen voor de deadline op 1 mei 2025, te worden verstuurd aan de toezichthoudende instantie, de Rijksdienst voor Identiteitsgegevens. Dit heeft tijdig plaatsgevonden.

Uit de uitgevoerde zelfevaluatie blijkt dat de gemeente Ooststellingwerf met een totaalscore van **90,5%** (vorig jaar 91,6%) vanuit de Kwaliteitsmonitor en een totaalscore van **97%** (vorig jaar 97%) vanuit ENSIA goed scoort op kwaliteit en veiligheid van het aanvraag- en uitgifteproces Paspoorten en Nederlandse identiteitskaarten. De gemeente Ooststellingwerf voldoet daarmee aan de wettelijke norm van **90%**.

Nadere onderzoeken RVIG - steekproef

De RvIG voert jaarlijks nadere onderzoeken uit om te bekijken of de uitkomsten van de zelfevaluaties van de BRP en PNIK een juiste afspiegeling vormen van de werkelijke situatie. Deze onderzoeken vinden plaats door middel van een steekproef bij ten minste 35 gemeenten. Desbetreffende gemeenten worden daarover dan na afloop van het verantwoordingsjaar geïnformeerd.

De RviG heeft ons geïnformeerd dat er een nader onderzoek op 23 mei 2025 gaat plaatsvinden over de door ons uitgevoerde zelfevaluatie BRP.

7.1 ICT beveiligingsassessments DigiD

Sinds 2013 moeten alle organisaties die DigiD gebruiken aan bepaalde beveiligingsrichtlijnen voldoen. De gemeente beschikt over 2 DigiD-aansluitingen welke onderdeel uitmaken van de zelfevaluatie middels ENSIA. Beide DigiD-aansluitingen maken onderdeel uit van de onafhankelijke ENSIA IT-audit en zijn opgenomen in de collegeverklaring ENSIA 2024. Voor beide DigiD aansluitingen voldoet onze gemeente aan de gestelde normen.

7.2 Suwinet

In het verleden zijn kritische inspectierapporten verschenen over de manier waarop gemeenten gebruik maken van Suwinet, het gegevensuitwisselingsysteem in het maatschappelijk domein voor Werk en Inkomen. De gemeente Ooststellingwerf scoorde voldoende op deze onderzoeken door de inspectie. Uit de onderzoeken bleek dat Suwinet zelf ook voor verbetering vatbaar was op het gebied van privacy en beveiliging. De VNG heeft het programma Borging Veilig Gebruik Suwinet opgezet om gemeenten te ondersteunen bij de implementatie van een zorgvuldige en veilige gegevensuitwisseling, onder meer door tools en maatregelen aan te reiken, en door accountmanagers te laten ondersteunen bij de implementatie van de verschillende maatregelen. Dit heeft geleid tot het implementeren van een fijnmazige autorisatie en gebruik van de zogenaamde ‘whitelist’ waarbij over de reden van de raadpleging in SUWI moet worden verantwoord door de gebruiker.

Suwinet maakt onderdeel uit van de onafhankelijke IT-audit en is opgenomen in de collegeverklaring ENSIA 2024. Het normenkader is met de invoering van de verantwoordingssystematiek middels ENSIA aangescherpt. Daar waar voorheen 7 essentiële normen in het onderzoek werden betrokken, zijn middels de zelfevaluatie 14 normen onderzocht. De gemeente Ooststellingwerf voldoet aan alle 14 normen.

7.3 Verantwoording BAG, BGT en BRO

De BAG (Basisregistratie Adressen en Gebouwen), de BGT (Basisregistratie Grootschalige Topografie) en de BRO (Basisregistratie Ondergrond) zijn een belangrijk onderdeel van het stelsel

van basisregistraties. Op basis van de resultaten uit de uitgevoerde zelfevaluaties is in aparte rapportages verantwoording afgelegd aan het college van B&W. Deze rapportages maken geen onderdeel uit van de IT audit; de scope van de IT audit omvat DigiD en SUWInet.

BAG
Op basis van de uitgevoerde zelfevaluatie blijkt dat de gemeente ruim voldoet aan de specifiek gestelde beveiligingsmaatregelen rond de administratieve inrichting van de BAG. Met een behaalde resultaat van **99%** (vorig jaar 92%) wordt ruimschoots voldaan aan de minimale norm van **75%**.

De wet BAG schrijft voor dat de definitieve pandgeometrie binnen zes maanden in de BAG registratie moet zijn geregistreerd.

Onze gemeente beschikt over een eigen landmeter. Hierdoor heeft de gemeente meer grip op de actualiteit van definitieve pandgeometrie. Dit heeft daarmee geleid tot een hogere score op het onderdeel gegevenskwaliteit.

BGT
Uit de zelfevaluatie blijkt dat de gemeente de uitvoering van het beheer en de kwaliteit van de BGT beheerst en waarborgt. Net als vorig jarig is in 2024 wederom volledig voldaan aan alle normen. De gemeente Ooststellingwerf heeft een **100%** score als resultaat waarmee ruimschoots wordt voldaan aan de minimale norm van **75%**.

BRO
Met ingang van het jaar 2019 is ook de uitvoer van de zelfevaluatie Basisregistratie Ondergrond (BRO) verplicht en is deze taak formeel belegd. In 2019 zijn er met betrekking tot de BRO voor het eerst stappen ondernomen. Inmiddels blijkt met de al uitgevoerde acties, dat de gemeente de uitvoering van de BRO beheerst en waarborgt. Bij de BRO is het mimimaal te behalen norm gesteld op **60%**. Met een score van **92%** (vorig jaar 89 %**)** voldoen we ruimschoots aan de norm. Wel is er sprake van een lagere score dan in 2021 en 2022, waar zelfs destijds sprake was van een **100%** score behaald. Dit is het gevolg van het steeds meer moeten registreren van objecten in de BRO. Door de uitbreiding zijn ook steeds meer disciplines betrokken bij de registratie en ligt de nadruk meer en meer op het actief blijven delen van de BRO en de plichten die wij hierin hebben.

WOZ
De Waarderingskamer heeft besloten om met ingang van het verantwoordingsjaar 2023 de vragen gericht op de uitvoering van de Wet WOZ niet meer op te nemen in ENSIA en deelname aan ENSIA vooralsnog te stoppen. Dit betekent dat sinds 1 juli 2023 in ENSIA geen vragen over de WOZ-uitvoering meer worden gesteld.

8 Beveiligingsincidenten en datalekken

De gemeente beschikt over een register van beveiligingsincidenten en datalekken welke gemeld zijn aan de beveiligingsfunctionaris (CISO) / Functionaris Gegevensbescherming (FG). Beveiligingsincidenten en datalekken worden centraal geregistreerd (in een beveiligde omgeving) en indien daarom gevraagd door de toezichthouder ter inzage verleend.

Een beveiligingsincident dient te worden gemeld aan de beveiligingsfunctionaris (CISO) / Functionaris Gegevensbescherming (FG). Deze beoordeelt of het beveiligingsincident kan worden aangemerkt als een datalek en of deze gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) en eventueel indien er sprake is van nadelige gevolgen voor de persoonlijke levenssfeer aan betrokkene(n). De beoordeling komt tot stand op basis van de meldplicht datalekken onder de AVG, het daarvoor ontwikkelde stroomschema en het vragenformulier. Met ingang van 2023 is de Wpg hierin geïntegreerd. De procedure rondom het melden van beveiligingsincidenten / datalekken is vastgesteld door de directie (**zie 5.1**).

De beveiligingsfunctionaris (CISO) / Functionaris Gegevensbescherming (FG) is gemandateerd om datalekken te melden aan de Autoriteit Persoonsgegevens (AP) en treedt op als contactpersoon. Hieronder volgt een overzicht van de incidenten in 2024 welke zijn gemeld aan de

beveiligingsfunctionaris (CISO) / Functionaris Gegevensbescherming (FG), waarbij er persoonsgegevens zijn gelekt en aldus beoordeeld als een datalek :

Datalek, geen melding aan de AP:

- **04/2024 Backoffice Sociaal Domein:** bestanden met facturen van Medipoint zijn per ongeluk naar een OWO-mailadres verzonden in plaats van in een separate mail. Hierdoor hebben de contractmanagers gegevens kunnen inzien van cliënten van de andere gemeenten. Omdat het gaat om een interne mailwisseling binnen OWO is er geen sprake van nadelige gevolgen voor de persoonlijke levenssfeer van betrokkenen. Ambtenaren hebben allen de verklaring ambtseed/-belofte afgelegd waardoor de integriteit is geborgd op basis waarvan geen melding aan de AP nodig is.

- **05/2024 Samenleving:** subsidieaanvraag openbaar in Ibabs. De aanvraag bevat enkel algemene persoonsgegevens (naam en adres). De aanvraag is alsnog geanonimiseerd waarmee het datalek is gedicht.

- **07/2024 Ruimte en Economie:** melding diefstal laptop en werktelefoon, usb en notitieboekje. De werktelefoon is voorzien van een inlogcode en de laptop is beveiligd met gebruikersnaam en wachtwoord. De kans is daarmee heel klein dat een onbevoegde beide heeft kunnen ontgrendelen en kennis heeft kunnen nemen van zakelijke gegevens op het werkgebied van de melder waarin gegevens van inwoners, instellingen zijn opgenomen. De verwerking van persoonsgegevens binnen het vakgebied zijn bovendien zeer algemeen van aard, waarmee geen nadelige gevolgen voor de persoonlijke levenssfeer voor inwoners valt te verwachten als deze ingezien zouden zijn. Ook de usb en het notitieboekje bevat geen gevoelige persoonsgegevens. Er is direct melding gedaan bij I&A en er is aangifte gedaan bij de politie. Er is daarmee geen melding noodzakelijk bij de AP.

- **07/2024 BKWI:** Bij het online aanvragen van een specifieke rapportage in SUWI-net met betrekking tot het gebruik van SUWI-mail zijn emailadressen inzichtelijk geweest van medewerkers van andere gemeenten en van onze medewerkers door anderen. Het datalek bevindt zich binnen de sector (betrouwbare omgeving/ontvangers) en het gaat hier enkel om zakelijke e-mailadressen van gemeentemedewerkers. Daarnaast kunnen alleen de gemandateerden binnen een gemeente de online rapportagemodule raadplegen/opvragen. BKWI heeft het probleem opgelost, waarmee het datalek is gedicht.

- **11/2024 Backoffice Sociaal Domein:** interne mail met klantgegevens van Ooststellingwerf per ongeluk verzonden naar een collega in Opsterland. Het gaat enkel om algemene persoonsgegevens (namen cliënten). Als gemeenteambtenaar hebben we allen de verklaring ambtseed-/belofte afgelegd en mag je van de ontvanger verwachten hier integer mee om te gaan. De mail is verwijderd, waarmee het datalek is gedicht.

- **12/2024 Backoffice Sociaal Domein:** interne mail met naam en BSN van een inwoner van de gemeente Ooststellingwerf is per ongeluk verzonden aan een collega in Opsterland. interne mail. Als gemeenteambtenaar hebben we allen de verklaring ambtseed-/belofte afgelegd en mag je van de ontvanger verwachten hier integer mee om te gaan. Daarnaast heeft de ontvanger de mail verwijderd waarmee het datalek is gedicht.

- **12/2024 BVI:** klacht betrekking op een inwoner van Opsterland m.b.t het werkterrein van BVI is ter behandeling doorgestuurd aan cluster BJZ in Ooststellingwerf. Omdat dit betrekking heeft op een inwoner van Opsterland, dient de klacht te worden behandeld door de gemeente waar desbetreffende inwoner is gehuisvest. De klacht had ter behandeling doorgestuurd moeten worden aan het juridisch cluster aldaar. Als gemeenteambtenaar hebben we allen de verklaring ambtseed-/belofte afgelegd en mag je van de ontvanger verwachten hier integer mee om te gaan.

- **12/2024 Gebiedsteam (domein WMO/Jeugd):** per ongeluk is bij een afgegeven beschikking in het kader van een WMO-voorziening een pasfoto meegezonden van een andere inwoner.

Omdat per ongeluk een pasfoto is meegezonden met naam en geboortedatum is er sprake van een datalek. Een pasfoto geeft informatie over ras/etniciteit en kan in bepaalde situaties daarmee als een bijzonder persoonsgegeven worden beschouwd. Er zijn echter daarop een aantal uitzonderingen. Dezelfde pasfoto is in een eerdere situatie gebruikt voor het verstrekken van een GPK. De gemeente gebruikt de pasfoto niet met als doel onderscheid te maken in ras/etniciteit. Elke inwoner heeft immers daarop recht als deze aan de voorwaarden voldoet. Het datalek is inmiddels gedicht doordat de inwoner die het heeft ontvangen bij de beschikking van de WMO-voorziening deze heeft teruggegeven. Er zijn dan ook geen nadelige gevolgen voor de persoonlijke levenssfeer te verwachten van degene die het betreft. Daarmee is melding aan de AP niet noodzakelijk.

Omdat er in voornoemde situaties over het algemeen geen sprake is van het lekken van bijzondere persoonsgegevens is melding aan de AP niet van toepassing. In situaties waarbij geen bijzondere persoonsgegevens zijn gelekt maar wel van het lekken van gevoelige informatie anderszins (zoals een BSN) is melding niet noodzakelijk indien er vooraf of achteraf passende maatregelen zijn getroffen, snel herstelacties hebben plaatsgevonden om het lek te dichten en intern binnen OWO is gebleven. Er zijn dan geen nadelige gevolgen voor de persoonlijke levenssfeer van betrokkene(n).

Datalek, melding aan de AP (en evt. aan betrokkene(n)):

- **08/2024 BVI:** ingevuld kwijtscheldingsformulier is per ongeluk verstuurd aan een andere bewoner. Dit formulier bevat naast algemene persoonsgegevens (naam, adres, woonplaats, contactgegevens, geboortedatum) ook persoonsgegevens van zeer gevoelige aard (BSN, bankgegevens, gegevens over financiële situatie). Daarom is er melding gedaan aan de AP. De ontvanger heeft direct contact opgenomen met de gemeente en aangegeven de mail te hebben verwijderd, waarmee het datalek is gedicht. Team BVI heeft de betrokkene per brief op de hoogte gesteld van dit datalek.

- **10/2024 GBT domein Werk en Inkomen:** een verklaring omtrent voortzetting bewind (ten behoeve van de rechtbank) is per ongeluk verstuurd naar een andere inwoner, als gevolg van het onjuist invoeren van het emailadres (typefoutje). Niet bekend is de mail daadwerkelijk bij een ander is terechtgekomen, geen onbestelbare retourmelding ontvangen, maar kan niet worden uitgesloten. Naast algemene persoonsgegevens (naam, adres, woonplaats, geboortedatum) bevat de brief ook gevoelige persoonsgegevens (gegevens over de financiële situatie). Gegevens over de financiële situatie kunnen leiden tot stigmatisering , reputatieschade van de persoon waarvan gegevens zijn gelekt. Daarom is melding gemaakt aan de AP. Daarnaast is betrokkene van wie gegevens zijn gelekt op de hoogte gesteld van dit datalek.

In alle voornoemde situaties is er sprake van het lekken van bijzondere persoonsgegevens of anderszins gevoelig van aard en melding aan de AP noodzakelijk en evt aan betrokkene(n). Omdat er herstelacties hebben plaatsgevonden zijn er geen ernstige nadelige gevolgen (waarbij inschatting verwaarloosbaar of beperkt) te verwachten voor de persoonlijke levenssfeer van betrokkene(n).