Rapportage informatieveiligheid en privacy

Periode 2018

Gemeente Ooststellingwerf

Datum : 01-05-2019

Auteur: Hans Siccama

Inhoudsopgave

1 VERSIEBEHEER 3

2 VERANTWOORDING 3

3 DOEL EN SCOPE 3

4 BELEID EN VERANTWOORDING 3

4.1 BELEID 3
4.2 ENSIA 4
4.3 VNG VISITATIECOMMISSIE INFORMATIEVEILIGHEID 6
4.4 WAAR STAAT JE GEMEENTE 7

5 PRIVACY 8

5.1 MELDPLICHT DATALEKKEN 9
5.2 VERWERKINGSREGISTER EN VERWERKERSOVEREENKOMSTEN 9
5.3 DATA PROTECTION IMPACT ASSESSMENT 9
5.4 RECHTEN VAN BETROKKENEN 10

6 DREIGINGEN, RISICO'S EN TRENDS 10

7 AUDITS, KWETSBAARHEIDSTESTEN EN STEEKPROEVEN 11

7.1 ICT BEVEILIGINGSASSESSMENTS DIGID 12
7.2 SUWINET 12
7.3 VERANTWOORDING BAG, BGT EN BRO 12

8 BEVEILIGINGSINCIDENTEN EN DATALEKKEN 13

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

2 Verantwoording

De rapportage wordt jaarlijks opgemaakt door de beveiligingsfunctionaris / functionaris gegevensbescherming 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 2018. 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 vanwege de ontwikkelingen van nieuwe wetgeving ten aanzien van bescherming van persoonsgegevens, de Algemene Verordening gegevensbescherming welke per 25 mei 2018 in werking is getreden..

4 Beleid en verantwoording

4.1 Beleid

In het gemeentelijke informatiebeveiligingsbeleid, laatstelijk door het college vastgesteld op 7 februari 2017, en geldend voor een periode van 3 jaar, is de Baseline Informatiebeveiliging Nederlandse Gemeenten (hierna BIG) 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 en BGT) zijn hierin grotendeels geïntegreerd.

Met de vaststelling van het algemene informatiebeveiligingsbeleid, de beleidsuitgangspunten en de verantwoordelijkheden voor de informatiebeveiliging stelt het college de kaders voor informatiebeveiliging vast. In de verantwoordelijkheden is opgenomen dat het onderliggende, flankerende beleid inclusief procedures, richtlijnen en beveiligingsmaatregelen vastgesteld worden door de directie. In 2018 is het informatiebeveiligingsbeleid geactualiseerd.

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. Het beleid hoe wij intern binnen de gemeente omgaan met privacy is, na instemming van de OR, vastgesteld door het college op 15 mei 2018. Daarnaast heeft de gemeente privacybeleid ontwikkeld voor onze burgers. Dit beleid samen met de privacyverklaring, is vastgesteld op 22 mei 2018 en gepubliceerd op onze gemeentewebsite. Het privacybeleid word ieder jaar geëvalueerd en indien nodig herzien.

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 de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" van 2013 hebben de gemeenten afgesproken de Baseline Informatieveiligheid Gemeenten (BIG) te implementeren. 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 in de paragraaf bedrijfsvoering.

Verticale verantwoording

Over de BRP, PUN, Suwinet, BAG, BGT, BRO en DigiD moeten gemeenten ook verantwoording afleggen. Dit noemen we de 'verticale verantwoording'. De horizontale verantwoording richting gemeenteraad vormt hiervoor de basis. De normen van de BIG en de specifieke normen van de BRP, PUN, Suwinet, BAG, BGT, BRO en DigiD zijn opgenomen in de zelfevaluatievragenlijst. Voor de zelfevaluatie Basisregistratie Ondergrond (BRO) geldt 2018 als een proefjaar. In deze vragenlijst zijn ook vragen opgenomen over niet-informatieveiligheidsaspecten, zodat deze niet op een apart moment hoeven te worden beantwoord.

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.

<u>Vragenlijst zelfevaluatie Informatieveiligheid</u>
De zelfevaluatie over informatieveiligheid over de volle breedte van de BIG 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 en W aan in hoeverre de beheersmaatregelen aan de van kracht zijnde beveiligingsnormen voldoen.

De scope van de IT-audit in 2018 heeft betrekking op DigiD en SUWI. Voor het jaar 2018 geldt dat de verantwoording Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius) wordt verantwoord door middel van een Collegeverklaring. De Collegeverklaring is opgesteld op basis van de bevindingen uit onze zelfevaluatie en getoetst door een IT-auditor.

De Collegeverklaring ENSIA 2018 omvat het op 31 december 2018 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.0).

Uit de Collegeverklaring ENSIA blijkt dat aan alle normen m.b.t. de DigiD-aansluitingen en SUWI wordt voldaan. De 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.

Ontwikkelingen 2019

Baseline informatiebeveiliging overheid (BIO)

Eén van de maatregelen om de informatieveiligheid bij de overheid te verhogen is de ontwikkeling van een gezamenlijk normenkader voor informatiebeveiliging voor alle overheidslagen: de Baseline Informatiebeveiliging Overheid.

Momenteel stellen overheden hun informatieveiligheidsbeleid vast aan de hand van een basisnormenkader, ook wel de baseline informatiebeveiliging genoemd. Het Rijk hanteert de Baseline Informatiebeveiliging Rijksdienst (BIR), de provincies de Interprovinciale Baseline Informatiebeveiliging (IBI), de waterschappen de Baseline Informatiebeveiliging Waterschappen (BIWA) en de gemeenten de Baseline Informatiebeveiliging Gemeenten (BIG).

De aanstaande Baseline Informatiebeveiliging Overheid (BIO) bundelt deze huidige afzonderlijke baselines per overheidslaag (Rijk, provincies, waterschappen en gemeenten) en kan worden beschouwd als de ‘kapstok’ waaraan de elementen van informatiebeveiliging per overheidslaag opgehangen kunnen worden.

Wat is de BIO?
De BIO betreft een doorontwikkeling, een ‘update , van de sectorspecifieke baselines, waaronder de nu bestaande BIG en biedt een uniforme basis om te zorgen dat de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid bevorderd wordt.
Gemeenten baseren hun informatiebeveiligingsbeleid en hun verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk (middels ENSIA) op deze BIG. De werkzaamheden die voor de BIG zijn verricht zijn overigens al grotendeels in lijn met de BIO.

Verschil : meer risicomanagement

De BIO legt meer nadruk op risicomanagement dan de BIG, die meer gaat over specifieke maatregelen. De rol van de bestuurder en lijnmanager is ten aanzien van risicomanagement explicieter dan de BIG aangaf. Om daaraan invulling te geven wordt tegelijkertijd met de BIO een handreiking ‘10 bestuurlijke principes voor informatiebeveiliging’ van kracht. Deze principes ondersteunen bestuurders bij de invulling van hun verantwoordelijkheid.

De BIO verschilt op een aantal punten van de BIG. De grootste verschillen zijn:

1.Minder maatregelen (bijna 60% minder)
2.Maatregelen zijn altijd verplicht
3.Meer risicomanagement (het begint met een QuickScan)
4.Er zijn 3 Basisbeveiligingniveaus (BBN)
5.Selectie van ontbrekende maatregelen vooraf
6.Toewijzing van maatregelen op eindverantwoordelijke
7.Een baselinetoets (QuickScan) die rekening houdt met die 3 niveaus

De grootste verandering zal zijn dat ook bijvoorbeeld ENSIA compleet opnieuw zal moeten worden ingericht en daar is heel wat werk te verzetten. Ook een grote verandering is dat de aanpak anders is dan bij de BIG en dat betekent ook een wijziging in het ondersteuningsaanbod van de Informatiebeveiligingsdienst door middel van operationele BIO-producten voor gemeenten.

Inwerkingtreding in 2020, overgangsjaar 2019
Het is de verwachting van alle overheidslagen dat de BIO op 1 januari 2020 van kracht wordt. In 2019 kunnen gemeenten zich voorbereiden op de overgang van de BIG naar de BIO. De informatiebeveiligingsdienst (IBD) ondersteunt gemeenten daarbij met producten en regionale bijeenkomsten. De verantwoordingssystematiek ENSIA zal ook worden bijgewerkt naar de BIO.

In het voorjaar van 2019 wordt de ENSIA vragenlijst aangepast en in een pilot ter beschikking gesteld aan een aantal gemeenten en toezichthouders.

4.3 VNG Visitatiecommissie Informatieveiligheid

In februari 2017 heeft de visitatiecommissie informatieveiligheid van de VNG de gemeente Ooststellingwerf bezocht. De aanbevelingen die de commissie naar aanleiding van dit bezoek heeft gedaan – zie opsomming hieronder - hebben geleid tot de volgende activiteiten:

1. Maak de raad structureel deelgenoot 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. De raad wordt daarnaast jaarlijks middels deze rapportage geïnformeerd.

2. Maak werk van informatieveiligheid door middel van sequentiële vervolgstappen op basis van een planmatige aanpak en stuur op de voortgang.

Ondernomen acties:
De gemeente heeft informatiebeveiligingsbeleid, vastgesteld d.d. 7 februari 2017, gebaseerd op de BIG. Er heeft inmiddels een GAP- en impactanalyse plaatsgevonden op de 133 beheersmaatregelen van de BIG; resultaat is dat we inzicht hebben in de status van informatiebeveiliging, actiehouders en planning. De uitkomsten hiervan worden te zijner tijd, na afloop van het verantwoordingsjaar 2018, rond me/juni 2019 geactualiseerd en verwerkt in de zogenaamde Verklaring van Toepasselijkheid (VVT) en onderliggend jaarplan. In de loop van 2019 zal er wederom een GAP- en impactanalyse plaatsvinden, echter gebaseerd op de BIO (zie 4.2 onder ontwikkelingen).

3. Besteed nadere aandacht aan het leveranciersmanagement.

Ondernomen acties:
Leveranciersmanagement maakt als norm onderdeel uit van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Met invoering van de Algemene Verordening Gegevensbescherming (AVG) zijn de eisen waaraan verwerkingen van persoonsgegevens moeten voldoen verscherpt. Onze gemeente beschikt over een privacy verwerkingsregister, centraal bijgehouden door de Functionaris Gegevensbescherming (FG). In dit register worden ook verwerkingen opgenomen die zijn uitbesteed aan leveranciers.

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 doorgevoerd als onderdeel van het startformulier in het inkoopbeleid.

4. Maak een bewerkersovereenkomst met de samenwerkende gemeenten.

Ondernomen acties:
In 2014 is de samenwerking tussen de drie gemeenten 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.

5. Aan het werk met een (leuk!) leerprogramma.

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.

De cyclus bestaat uit acties in het kader van leren, begeleiden en ontwikkelen van 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 de 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 (huidige samenstelling).

Informatieveiligheid en privacy zijn derhalve thema's die doorlopend aandacht verdienen. Beveiligd mailen via Cryptshare, 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 in 2018 heeft getroffen om de kans op een datalek te verkleinen.

De volgende in te zetten acties staan voor het jaar 2019 gepland om in te zetten:

1. Presentatie door SEP over informatiebeveiliging en privacy aan het college;
2. Lunchbijeenkomst in de raadszaal (duur 1 uur en 30 minuten): Peter Zinn is internationaal spreker, inspirerend en spraakmakend, met 10 jaar ervaring als cybercop bij het Team High Tech Crime van de politie. Vanuit die ervaring heeft hij vele levendige verhalen en spannende voorbeelden over cybercrime en cybersecurity die hij graag met ons wil delen;
3. E-learning Privacy (3 modules) en datalekken (1 module); gehele organisatie inclusief raadsleden;
4. Inzet Mystery Guest door SEP.

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

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 naam 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). Beiden zijn aangemeld bij de Autoriteit Persoonsgegevens..

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.

Op grond van de Wet op de ondernemingsraden heeft de OR instemmingsrecht over het privacy beleid voor zover het interne toezicht de gegevensbescherming van het personeel raakt. Op 26 april 2018 heeft de OR ingestemd met het privacy beleid en de taken, verantwoordelijkheden en bevoegdheden zoals vastgelegd in het Reglement Functionaris voor de gegevensbescherming, vastgesteld door het college op 15 mei 2018.

Per 25 mei 2018 voldoet de gemeente aan de volgende minimale gestelde 6 AVG-maatregelen, zoals eerder aangegeven in een ledenbrief van de VNG:

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.

5.1 Meldplicht datalekken

Al sinds 1 januari 2016, maar ook onder de AVG, 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 zijn gelekt (gegevens van gevoelige aard) en 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 vastgesteld met daarin een stroomschema voor het melden en afhandelen van een datalek. De beveiligingsfunctionaris / functionaris gegevensbescherming 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 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 zijn opgenomen in het verwerkingsregister. Hierin 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 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. In dat geval 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 DPA 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.

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 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, vastgesteld door de directie op 5 juni 2018. Daarin is ook de rol van de privacy functionaris opgenomen, verantwoordelijk voor de afhandeling van inzageverzoeken.

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

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[1] 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 inbreuk 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).

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.

Vanaf 2018 publiceert de IBD het Dreigingsbeeld voor Nederlandse gemeenten. Het dreigingsbeeld is geschreven voor het management. De inhoud van het dreigingsbeeld wordt door de beveiligingsfunctionaris (CISO) omgezet in een actieplan indien nodig.

7 Audits, kwetsbaarheidstesten en steekproeven

In 2018 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 PUN 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 ingelezen in de Kwaliteitsmonitor en samengevoegd met de antwoorden op de BRP/PNIK-vragenlijst en verwerkt in managementrapportages. 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% (norm = 90 %) voldoende scoort op de inrichting, de werking en de beveiliging van de basisregistratie Personen.

Zelfevaluatie PNIK (waardedocumenten)

Op grond van de Paspoortuitvoeringsregeling Nederland 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 zijn tijdig verstuurd aan de toezichthoudende instantie, de Rijksdienst voor Identiteitsgegevens. Uit de uitgevoerde zelfevaluatie blijkt dat de gemeente Ooststellingwerf met een totaalscore van 93,7 % 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%.

In maart/april 2019 zijn er door de RvIG nadere onderzoeken uitgevoerd om te bekijken of de uitkomsten van de zelfevaluaties van de BRP en PNIK een juiste afspiegeling vormen van de werkelijke situatie. Deze onderzoeken zullen weer plaatsvinden door middel van een steekproef bij ten minste 35 gemeenten. De gemeente Ooststellingwerf is in 2 achtereenvolgende jaren in de steekproef gevallen en is daarom in 2019 (verantwoording over het jaar 2018) niet in de steekproef getrokken.

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 opgenomen in de collegeverklaring ENSIA 2018. Voor beide DigiD aansluitingen voldoet onze gemeente aan de gestelde normen.

7.2 Suwinet

De afgelopen jaren 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 verantwoordt door de gebruiker.

Suwinet maakt onderdeel uit van de onafhankelijke IT-audit en is opgenomen in de collegeverklaring ENSIA 2018. Het normenkader is als gevolg van ENSIA aangescherpt. Daar waar voorheen 7 essentiële normen in het onderzoek werden betrokken, zijn middels de zelfevaluatie 13 normen onderzocht. De gemeente Ooststellingwerf voldoet aan alle 13 normen.

7.3 Verantwoording BAG, BGT en BRO

De BAG (Basisregistratie Adressen en Gebouwen) en de BGT (Basisregistratie Grootschalige Topografie 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 de gemeenteraad. Deze rapportages maken geen onderdeel uit van de IT audit; de scope van de IT audit omvat DigiD en SUWInet.

Op basis van de uitgevoerde zelfevaluatie blijkt dat de gemeente niet volledig voldoet aan de specifiek gestelde beveiligingsmaatregelen rond de administratieve inrichting van de BAG, wel wordt voldaan aan de minimale norm van 75%.

Ook blijkt dat de gemeente de uitvoering van het beheer en de kwaliteit van de BGT beheerst en waarborgt. De BGT is een vrij recente taak en zal zich door ontwikkelen tot het jaar 2020. Een maximale score hier is daarom logischerwijs nog niet mogelijk, maar zijn ten opzichte van het vorig jaar zichtbaar verbeteringen doorgevoerd. Aan de minimale norm van 75 % is voldaan.

Met ingang van het jaar 2018 is de uitvoer van een eventuele zelfevaluatie Basisregistratie Ondergrond (BRO) nieuw. Binnen de gemeente hebben we op dit onderdeel in 2018 echter nog geen stappen ondernomen. Het jaar 2018 is een proefjaar, de uitvoer van de zelfevaluatie is derhalve niet verplicht. Formeel is deze taak nog niet belegd, dit zal in de loop van 2019 plaatsvinden. Met ingang van het jaar 2020 zal ook verantwoording worden afgelegd over de BRO.

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 beoordeeld samen met de melder 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. De procedure rondom het melden van beveiligingsincidenten / datalekken is in juli 2017 vastgesteld door de directie.

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 2018 welke zijn gemeld aan de beveiligingsfunctionaris (CISO) / Functionaris Gegevensbescherming (FG) en waarbij er persoonsgegevens zijn gelekt en aldus beoordeeld als een datalek :

<u>Datalek, maar geen melding aan de AP:</u>

- BVI: verzonden mail, onjuist geadresseerde, met daarin de volgende persoonsgegevens: naam, adres, woonplaats en WOZ waarde (openbaar).
- GBT extern: verzonden mail, onjuist geadresseerde, met daarin de volgende persoonsgegevens: naam , adres, woonplaats van cliënt, namen en geboortedata van de kinderen.
- VTH: verzonden vergunning met begeleidende brief waarin naam, adres en woonplaats van een ander persoon.

Omdat er in voornoemde situaties geen sprake van het lekken van gevoelige (bijzondere) persoonsgegevens is melding aan de AP niet van toepassing. In alle situaties heeft er bovendien een herstelactie plaatsgevonden waardoor het lek is gedicht. Er zijn geen nadelige gevolgen voor de persoonlijke levenssfeer van betrokkenen.

<u>Datalek, melding aan de AP, maar in een later stadium ingetrokken:</u>

- GBT intern: zoekraken aanvraagformulier ziektekosten, met daarin de volgende persoonsgegevens: naam, adres, woonplaats, geslacht, geboortedatum, nationaliteit, BSN.
- GBT intern: zoekraken belastbaarheidsonderzoek met daarin de volgende persoonsgegevens: naam, adres, woonplaats, geslacht, geboortedatum, nationaliteit, BSN en bijzondere (o.a. vertrouwelijke medische) persoonsgegevens.

In voornoemde situaties kan niet met zekerheid worden uitgesloten dat er persoonsgegevens van gevoelige aard zijn gelekt en is melding, binnen 72 uur, gedaan aan de Autoriteit Persoonsgegevens.

De documenten zijn zoekgeraakt, ergens binnen de eigen gemeente, waarmee niet kan worden uitgesloten dat onbevoegden kennis hebben kunnen nemen van de inhoud. Binnen de gemeente wordt echter de verklaring ambtseed/belofte cq. schriftelijk integriteit afgelegd/ondertekend en de kans dat dit dan ook nadelige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkenen, wordt dan ook als zeer klein geacht. In een later stadium zijn de zoekgeraakte documenten echter teruggevonden, op basis waarvan de melding aan de AP is ingetrokken.

<u>Conclusie en advies</u>:
Uit het onderzoek van de Functionaris Gegevensbescherming (FG) blijkt dat er een grote achterstand is opgetreden in het archiveren/inscannen van de documentatie in Decos. De kans dat stukken met (gevoelige) persoonsgegevens zoekraken is reëel. De bescherming van de persoonsgegevens zijn binnen het proces niet voldoende gewaarborgd. Niet alleen is er in dergelijke situaties mogelijk sprake

van een datalek, ook kan niet worden voldaan (of niet tijdig) aan het afhandelen van verzoeken in de zin van de AVG wanneer betrokkene een beroep doet op de privacy rechten (inzage, correctie, verwijdering etc). Het niet kunnen voldoen aan de AVG kan leiden tot boetes.

De gemeente dient passende technische en organisatorische maatregelen te treffen om dit in de toekomst te voorkomen. De Functionaris Gegevensbescherming heeft geadviseerd maatregelen te treffen om de achterstanden m.b.t. de archivering spoedig weg te werken, hierop zijn inmiddels acties ondernomen..

Datalek, melding aan de AP:

- BVI: postpakket met bezwaarschriften WOZ en concept uitspraken kwijtgeraakt en geopend geretourneerd aan de gemeente. Het betreft een drietal inwoners van personen van de gemeente Opsterland met daarin de volgende persoonsgegevens: naam, adres, woonplaats, BSN en WOZ waarde (niet openbaar).

Omdat er in deze situatie sprake is van het lekken van gegevens van gevoelige aard is melding gedaan aan de Autoriteit Persoonsgegevens. De melding aan de betrokkenen is achterwege gelaten omdat het niet waarschijnlijk is dat het ongunstige gevolgen heeft voor de persoonlijke levenssfeer van betrokkenen. Het pakket is door een burger in een zeer kort tijdbestek terugbezorgd.

Het gaat om persoonsgegevens van een drietal inwoners van de gemeente Opsterland. Op basis van de regeling gezamenlijke verantwoordelijkheid OWO is het desondanks aan Functionaris Gegevensbescherming van de Gemeente Ooststellingwerf om de melding te doen aan de Autoriteit Persoonsgegevens. De Functionaris Gegevensbescherming heeft de gemeente Opsterland hierover ingelicht.