JAARRAPPORTAGE GEGEVENSBESCHERMING
Gemeenten Stede Broec, Enkhuizen en Drechterland
SED organisatie
2019 - 2020

Paul Gijben
Functionaris Gegevensbescherming
25 september 2020
Versie: 1.2

Samenvatting

Op 25 mei 2018 werd de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG verving de Wet bescherming persoonsgegevens (Wbp) en zorgt voor een verhoogde aandacht voor een rechtmatige verwerking van persoonsgegevens in alle sectoren. De overheid heeft hierin een belangrijke voorbeeldfunctie.

De colleges zijn verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens binnen de gemeenten. Dit brengt verplichtingen met zich mee. In deze jaarrapportage staat beschreven welke acties en maatregelen de gemeenten vanaf medio 2019 tot medio 2020 hebben genomen om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen. Ook bevat dit document aandachtspunten en actiepunten voor de aankomende jaren. Adequaat omgaan met persoonsgegevens is een continue proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

Samenvattend zijn de gemeenten voortgegaan met de privacy en gegevensbescherming waar zij begin 2019 waren gebleven. Voor nieuwe contractanten zijn verwerkersovereenkomsten afgesloten en constateer ik dat de weg richting de FG goed wordt gevonden. Er wordt in toenemende mate vragen gesteld over de toepasbaarheid van privacy binnen bepaalde processen of specifieke thema's. De taakvelden/aandachtsgebieden als WMO, jeugd en OOV zijn de grootste groep bevragers. Hier speelt privacy ook een belangrijke rol.

Specifieke aandacht blijft nodig om de (werk-)processen in beeld te brengen en vast te leggen, zodanig dat informatiestromen bekend zijn of worden. Enerzijds geeft dat een duidelijk beeld in wat er gedaan wordt en waar eventuele maatregelen m.b.t. privacy en gegevensbescherming nodig zijn, anderzijds biedt het de mogelijkheid voor een betere vastlegging en de daaraan gerelateerde zaken als: dataclassificatie, beheersbaarheid, kwaliteitsverbeteringen, werkinstructies etc. Hier wordt nog onvoldoende in geïnvesteerd, waardoor de groei in 'volwassenheid' op deze onderdelen achter blijft.

Het melden van informatiebeveiligingsincidenten lijkt nog steeds beperkt. Weliswaar zijn het aantal meldingen vanuit onze organisaties vergelijkbaar met het landelijk gemiddelde, maar lijkt dit slechts het topje van de ijsberg. Reden hiervoor is dat niet alle incidenten als zodanig worden herkend. Er is voldoende 'veiligheid' om incidenten te melden. Het merendeel van de meldingen betreffen mails of brieven naar verkeerd adres. Ook dat is landelijk gezien 'standaard'.

Inhoudsopgave

Inleiding

De gemeenten dienen zorgvuldig om te gaan met persoonsgegevens. Immers, zij werken met veel vertrouwelijke informatie. Niet alleen persoonlijke informatie van 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 dienen de gemeenten transparant te zijn welke persoonsgegevens zij verwerken en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. Bovendien moeten de gemeenten passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan. Daarnaast hebben de gemeenten te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen bij en van gemeenten.

Onder de verantwoordelijkheid van de colleges vinden een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om persoonsgegevens van inwoners van de gemeenten, belanghebbende, zakenrelaties en medewerkers. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dienen de gemeenten te beschikken over een interne toezichthouder: de Functionaris voor de Gegevensbescherming (FG). Op 1 maart 2018 hebben de colleges van de gemeenten Stede Broec, Enkhuizen, Drechterland en de SED directie Paul Gijben aangesteld als FG voor de separate gemeente en de SED organisatie.

De FG ziet erop toe dat de AVG intern wordt nageleefd. De colleges van de gemeenten en de SED directie dienen erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden 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 FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden en bevindingen en doet hij naar aanleiding daarvan aanbevelingen. Dit jaarverslag is bedoeld voor de colleges van de gemeenten Stede Broec, Enkhuizen, Drechterland en de directie/management van de SED organisatie. Na vaststelling van dit verslag zal dit ter informatie worden aangeboden aan de gemeenteraden van de bovengenoemde gemeenten, voorzien van een Raadsbrief.

Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen.
In het eerste deel wordt teruggekeken naar de afgelopen periode (medio 2019 – medio 2020). Wat hebben de gemeenten bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG? In het tweede deel worden aanbevelingen gedaan om gegevensbescherming en privacy voor het jaar (medio 2020 – medio 2021) naar een nog hoger niveau te tillen. Hierbij wordt, waar nodig, tevens aandacht geschonken aan de technische en organisatorische middelen die nodig zijn om dit hogere niveau te bereiken.

De criteria die in beide delen worden genoemd zijn afkomstig uit het document ‘Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie’ van de Informatiebeveiligingsdienst (IBD). In dit document worden criteria en maatregelen omschreven die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. In bijlage 1 is een overzicht opgenomen waar middels cirkeldiagramvorm wordt aangegeven in hoeverre de gemeenten en SED organisatie deze criteria hebben geïmplementeerd.

Deel 1. Terugblik op 2019 - 2020

Waar in 2018 - 2019 het accent lag om de AVG te implementeren is 2019 - 2020 de periode geweest van verdere optimalisatie en doorontwikkeling (privacy by design).

1. Het privacybeleid

Het privacybeleid is een kader waarin de gemeenten aangeven aan welke principes zij zich houden bij de verwerking van persoonsgegevens. Het laat zien hoe de gemeenten omgaan met persoonsgegevens en welke maatregelen zij treffen om te voldoen aan de relevante wet- en regelgeving.

Het privacybeleid gebaseerd op de AVG is nog in de maak. Medio maart 2020 is deze ter toetsing voorgelegd aan de juridische afdeling. Aansluitend wordt deze aan de OR aangeboden ter instemming. In het 3e kwartaal wordt het nieuwe privacybeleid ter vaststelling aangeboden aan de directie SED , vervolgens aan het Algemeen Bestuur en daarna aan de colleges van de separate gemeenten.
P&O heeft het personeelsreglement, waarin het onderdeel privacy is meegenomen, wel reeds laten vaststellen. Hierin zijn gedragscodes opgenomen met betrekking tot privacy aangaande de medewerker.

2. Processen

De verwerkingen van persoonsgegevens binnen de gemeenten dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kunnen de gemeenten in bepaalde gevallen verplicht zijn om een gegevensbeschermingseffectbeoordeling (DPIA[1]) uit te voeren.

Eind 2017 en begin 2018 zijn voor de risico-volle processen DPIA's uitgevoerd. Vanaf medio 2019 zijn voor nieuwe processen en projecten, ook op regionaal niveau, DPIA's uitgevoerd. Deze DPIA's zijn vastgelegd en beoordeeld door de FG. In bijlage 2 is een lijst van uitgevoerde DPIA's opgenomen.

3. Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat een ieder binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

Binnen het informatiebeveiligingsbeleid en het informatiebeveiligingsplan 2018 – 2019 is vastgesteld dat afdelingshoofden verantwoordelijk zijn voor informatiebeveiliging en privacy binnen de eigen afdeling/taakvelden. Begin 2020 zijn er aanvullende sessies over informatiebeveiliging en privacy gehouden. Dit betrof een open inschrijving waarop alle medewerkers konden aanhaken. Van de ca. 450 medewerkers hebben 75 medewerkers deze awareness-sessies daadwerkelijk gevolgd. Dit betreft dus bijna 17%.
Een grote tegenvaller hierbij is dat van de 75 medewerkers er slechts 2 teamleiders zich hadden aangemeld. Directie, afdelingshoofden en het merendeel van de teamleiders hebben zich niet aangemeld, terwijl zij wel verantwoordelijk zijn voor informatiebeveiliging en privacy binnen hun afdeling/taakveld (zie boven). Het gemis aan kennis op deze thema's kan leiden tot onjuiste keuzes of het onvoldoende kunnen beoordelen van belangrijke issues welke er kunnen spelen op het gebied van privacy en informatiebeveiliging.

4. Rechten van betrokkenen

De gemeenten (verantwoordelijken) dienen degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en - verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om controle en invloed uit te oefenen over het verwerken van zijn of haar persoonsgegevens.

Het is goed om te benoemen dat de mogelijkheid geboden wordt om digitaal een inzageverzoek in te dienen middels DigID. Hierbij wordt direct het identificatie-proces juist doorlopen.
Er zijn vanaf 2019 totaal 5 aanvragen voor inzage binnen gekomen en 1 aanvraag tot verwijdering van persoonsgegevens met betrekking tot rechten van betrokkenen. De inzage-verzoeken zijn allen afgehandeld door

[1] De gegevensbeschermingseffectbeoordeling wordt ook wel afgekort tot DPIA naar de Engelse term Data Protection Impact Assessment.

het digitaal aanleveren van de gevraagde documenten. De aanvraag van verwijdering is momenteel geëscaleerd via juridische weg. Hierbij is in beginsel ook de afdeling Juridische Zaken betrokken.

Ook actieve informatie is gehanteerd. In kader van de (behoorlijke) veranderingen op gebied van e-depot en Centrale Digitalisering Documenten ('scanstraat'), zijn de inwoners in de regio Westfriesland hiervan op de hoogte gesteld middels een schrijven op de websites van de regionale gemeenten.

5. Samenwerking

Gemeenten werken op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De gemeenten dienen dan ook afspraken te maken met deze andere partijen.

De samenwerkingspartijen zijn in 2018 voor het overgrote deel geïnventariseerd en beoordeeld door (externe) PO en FG op zijnde 'verantwoordelijke' of 'verwerker'. Dit is gebaseerd op de "Handleiding Algemene Verordening Gegevensbescherming en uitvoeringswet Algemene Verordening Gegevensbescherming" van het ministerie van Justitie en Veiligheid. De beslisboom is opgenomen in bijlage 3.
Met een groot aantal partijen is een verwerkingsovereenkomst getekend. Daarnaast zijn er diverse convenanten afgesloten welke afspraken omvatten hoe om te gaan met gegevensdeling en de privacy-aspecten. Op zich is een convenant géén grondslag om gegevens te mogen delen, doch 'slechts' aanvullende afspraken op een rechtmatige verwerking.
Verwerkersovereenkomsten blijven een punt van aandacht. Bij nieuwe contracten of afspraken zal overwogen moeten worden of een verwerkersovereenkomst noodzakelijk is. Nog niet altijd wordt deze stap meegenomen binnen de inkoop-procedure. Naast de nodige aandacht bij het taakveld 'inkoop' zal dit ook duidelijk op het netvlies moeten komen van afdelingen/taakvelden.

6. Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeenten passende technische en organisatorische maatregelen nemen ter beveiliging van persoonsgegevens. Hierbij dient te worden aangegeven dat op technisch beveiligingsgebied de gemeenten voor een groot deel afhankelijk zijn van de technische ICT ondersteuning welke door SSC DeSom wordt vorm gegeven. Dit richt zich op de normstelling van de BIG (Baseline Informatiebeveiliging Gemeenten), welke in 2020 vervangen zal zijn door de BIO (Baseline Informatiebeveiliging Overheid).
Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

Er zijn vanaf 1 juli 2019 t/m 30 juni 2020 in totaal 11 datalekken gemeld door medewerkers van de gemeenten (S, E, D en SED tezamen). Hiervan zijn er 4 meldingen aan de AP doorgeven, omdat zij een hoger risico kennen en hierdoor mogelijk een nadelig effect zouden kunnen hebben voor de betrokkene(n). De gemelde datalekken zijn niet toe te schrijven aan de gemeenten op zich. Het betreft hierbij menselijke handelingen vanuit de uitvoeringsorganisatie (SED).
Het aantal meldingen per gemeente ligt daarmee onder het landelijke gemiddelde m.b.t. lokale overheden. Het type/aard van de meldingen vertoond wel een sterke gelijkenis met het landelijk gemiddelde. In verreweg de meeste gevallen gaat het om mail of brief aan verkeerde afzender, dan wel met een verkeerde bijlage (voor een ander bestemd). Hierbij gaat het om 1 op 1 verkeer en geen 'bulk-post'.

Hoewel het aantal datalekken erg beperkt lijkt is dit juist een mogelijk probleem. Ontgaan datalekken ons? Worden datalekken (bewust) niet gemeld? Bestaat er een voldoende 'veilige omgeving' om datalekken te melden? Er is meer onderzoek nodig om inzicht te krijgen in deze materie.

In bijlage 4 is een overzicht opgenomen van de gemelde informatiebeveiligingsissues en beoordeelde datalekken vanaf medio 2019.

7. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat de colleges van de gemeenten Stede Broec, Enkhuizen en Drechterland moeten kunnen aantonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

Middels de jaarlijkse ENSIA beveiligingsrapportages en de jaarlijkse privacy rapportage verkrijgen de colleges inzage in de status van informatiebeveiliging en privacy. Daarnaast worden bij grote calamiteiten op informatiebeveiliging (en privacy) de colleges separaat geïnformeerd.
Directie en management dient dit regulier op te nemen in hun agenda. Hiertoe kunnen zij periodiek de FG en CISO uitnodigen om de status van privacy en informatiebeveiliging toe te lichten. Anderzijds kunnen FG en CISO ongevraagd, zeker als de noodzaak hiertoe is, informatie verstrekken aan Directie en management ten einde privacy en informatiebeveiliging, als een belangrijk onderdeel van de bedrijfsvoering en dienstverlening, als een continue aandachtspunt te belichten.

8. Conclusie

Vanaf medio 2019 hebben de gemeenten de lijn van 2018 voortgezet. Er is niet direct sprake van optimalisatie. Ook is de term ‘privacy by design’ (uit de AVG) nog niet omgezet naar daden. Wel kan worden gesteld dat de AVG geen onbekende factor meer is. Er komen veel vragen van medewerkers binnen, vooral van de taakvelden uit het sociaal domein (WMO, jeugd) en OOV, met name over het delen van gegevens met andere medewerkers, inwoners en/of derden.

Speciale aandacht verdient de uitwisseling van gegevens met omringende gemeenten en werkorganisaties. In bepaalde gevallen is er sprake van het handhaven van een uiterst streng beleid bij deze partijen. Dat de wet gehandhaafd dient te worden spreekt, maar het mag niet leiden tot het blokkeren van gemeente-specifieke processen dan wel het beoordelen op halve informatie. Het gesprek zou hierover moeten worden aangegaan op bestuurlijk niveau.

De AVG blijft een lastige wetgeving waarbij enerzijds ‘het voldoen aan wet- en regelgeving’ en anderzijds ‘het operationeel houden van de huidige processen’ spelen. Privacy is geen doel op zich, doch een kwaliteitsmechanisme welke, conform wetgeving, in de loop der tijd ‘als vanzelf verloopt’. In sommige gevallen betekent dat er nog gedraaid moet worden aan de ‘afstelknoppen’ en een balans moet worden gevonden tussen werkbaarheid en privacyproof.

Ook dient te worden opgemerkt dat de huidige invulling van de privacy vanaf medio 2019 geen organisatie-issue was. Het beperkt zich tot een aantal medewerkers. Dit betreft wel een zorg punt. Privacy dient meer ingebed te worden als onderdeel binnen het bedrijfsproces. Hetzelfde geldt voor informatiebeveiliging. Beide onderdelen verdienen meer aandacht vanuit directie en management.

In bijlage I zijn tabellen opgenomen welke inzicht geven in de status van de privacy uitvoering binnen de SED organisatie. Deze tabellen komen tot stand middels een uitgebreide vragenlijst op de diverse benoemde categorieën. Op alle vragen bestaat de mogelijkheid tot de antwoorden:

- Ja
- Nee
- Deels
- Niet van Toepassing
- Onbekend

<u>Duiding</u>
In alle categorieën is er sprake van vragen in een ‘oplopende kwaliteit’. We voldoen in alle categorieën aan de minimale vereisten en scoren merendeels tot 75% (ruim voldoende). De beantwoording ‘deels’ geeft aan dat het noch volledig ‘ja’ dan wel ‘nee’ is. De mate van ‘deels’ wordt niet gevraagd en dus niet gescoord.

Uiteraard dienen we telkens te optimaliseren en hierdoor een kritische blik te werpen op die onderdelen welke nog onvoldoende scoren. Deze rapportage, en zeker waar het gaat om die aspecten die specifiek belicht worden, geven invulling aan die kritische noot.

Deel 2. Vooruitkijken naar 2020 - 2021

Gegevensbescherming onderdeel laten worden van de organisatie, en daarmee aantoonbaar voldoen aan de relevante wet- en regelgeving, is geen afvinklijst, maar een continu proces. Het vraagt om structurele borging van dit onderwerp. Waar het jaar 2019 in het teken stond van verdere optimalisering van de privacy en gegevensbescherming, zal vanaf medio 2021 meer in het teken moeten staan van verdere doorontwikkeling; basis op orde en het meer gaan toepassen van 'privacy by design'.

1. Het privacybeleid

Aanbevelingen:

1) Het binnenkort uitgebracht herziene privacybeleid m.b.t. AVG vaststellen (SED Directie en separate colleges).

Ad 1) Deze formaliteit zal 3e kwartaal 2020 worden doorgevoerd. Momenteel ligt het beleid voor aan de OR, omdat ook de privacy van de medewerker hierin wordt meegenomen.
Niet onbelangrijk is de vindbaarheid van beleidsdocumenten, processen, procedures, protocollen, werkinstructies en richtlijnen in het algemeen. In brede context is dit onvoldoende. Op zich is deze stap niet moeilijk vorm te geven. Het combineren van al deze documenten in een overzichtelijke lijst met hyperlinks naar het desbetreffende document zal een goede basis vormen om (nieuwe) medewerkers hierop te kunnen attenderen. Het helpt de (nieuwe) medewerker zijn werk, conform hetgeen is afgesproken binnen de organisatie, te verrichten.

2. Processen

Aanbevelingen:

1) Standaard voor nieuwe processen en bij (regionale) projecten een DPIA uit te (laten) voeren;
2) Herijken van DPIA's bij risico-volle processen.

Ad 1) Voor nieuwe processen of (regionale)projecten, waarin persoonsgegevens worden verwerkt en dus een privacy-element geldt, een DPIA (laten) uitvoeren. DPIA's brengen de risico's binnen processen in beeld waar maatregelen voor genomen kunnen worden. Enerzijds draagt het bij om te kunnen voldoen aan wet- en regelgeving, anderzijds draagt het bij aan een verbetering van (proces-)kwaliteit.

Ad 2) Algemeen wordt gesteld dat DPIA's voor risico-volle processen om de 3 jaar herijkt moeten worden
Het herijken van reeds uitgevoerde DPIA's zal per 3 jaar opnieuw plaats moeten vinden, zodanig, dat er sprake is van een Plan-Do-Check-Act mechanisme. Vanaf medio 2020 zal hierdoor een groot deel van de in 2017 gehouden DPIA's opnieuw moeten worden uitgevoerd. Gaat dan met name om processen in het sociaal domein.

3. Organisatorische inbedding

Aanbevelingen:

1) Zorg te dragen dat privacy (maar ook informatiebeveiliging) standaard op de agenda komt te staan van management, directie en besturen;
2) Zorg te dragen dat (voor de nieuwe topstructuur) teamleiders verantwoordelijk zijn voor informatiebeveiliging en privacy binnen het eigen taakveld en de medewerkers hierin begeleiden/ondersteunen.

Ad 1) Om zorg te dragen dat privacy en informatiebeveiliging op de agenda komen te staan van het directie- en managementoverleg kunnen, periodiek (per kwartaal), de CISO en FG uitgenodigd worden om de status van privacy en informatiebeveiliging toe te lichten.

Ad 2) De colleges hebben middels het informatiebeveiligingsplan 2018 – 2019 vastgesteld dat afdelingshoofden verantwoordelijk zijn voor informatiebeveiliging en privacy binnen de eigen afdeling. Een mogelijke wijze om dit te bevorderen en meer inhoud te geven, is om bij afdelings- en/of taakveldoverleggen de CISO en/of FG hiervoor uit te nodigen. Voordeel hierbij is dat het afdelingshoofd wordt meegenomen in de vragen die er leven op afdelings- of taakveldniveau en dat er specifieker op de eigen afdelingsproblematiek kan worden ingezoomd.

4. Rechten van betrokkenen

Aanbevelingen:

1) Zorg te dragen dat medewerkers meer op de hoogte zijn cq. op de hoogte worden gesteld van beleid en procedures rondom de rechten van betrokkenen.

Ad 1) Medewerkers dienen meer op de hoogte te zijn van het beleid en de procedures rondom de rechten van betrokkenen (art. 11 t/m 22 AVG). De verzoeken van inwoners (vb. inzage-verzoek) worden niet altijd op de juiste wijze aangeleverd. De AVG stelt echter dat de organisatie hiervoor de nodige maatregelen dient te nemen zodanig dat waar of hoe een verzoek wordt gedaan dit herkend moet worden en in behandeling dient te worden genomen binnen gestelde termijnen (conform bestuursrecht). Het is derhalve van belang dat alle medewerkers van de organisatie hiervan op de hoogte zijn, verzoeken herkennen en naar de juiste plaats binnen de organisatie kunnen routeren. Deze aanbeveling sluit nauw aan op het gestelde onder punt 1 (Privacybeleid). Dit punt zou kunnen worden opgenomen met communicatie.

5. Samenwerking

Aanbevelingen:

1) Zorg te dragen dat bij iedere inkoopprocedure, waarbij een element van privacy is opgenomen, deze voorzien is van een motivatie over het al dan niet meegeven van een verwerkersovereenkomst, mede-verwerkersovereenkomst of overeenkomst gezamenlijke verwerking

Ad 1) Voor al die contractafhankelijke onderdelen dient, waar nodig, een privacy-overeenkomst aan te hangen. Om te bepalen óf dit nodig is én welke vorm van toepassing is kan de beslisboom vanuit de “Handleiding Algemene Verordening Gegevensbescherming en uitvoeringswet Algemene Verordening Gegevensbescherming” van het ministerie van Justitie en Veiligheid als leidraad dienst doen (bijlage 3). Deze zou ingebed moeten zijn in de algemene inkoop-procedure.

6. Beveiliging

Aanbevelingen:

1) Een duidelijk beleid en concrete afspraken (laten) vastleggen over het gebruik van ad-hoc communicatie.

Ad 1) De NTA-7516 norm is actief, wat betekent dat alle vormen van ad-hoc communicatie waarin medische of categorieën van medische gegevens staan, beveiligd dienen te worden met encryptie techniek. Hiervoor is begin 2020 gestart met de applicatie CryptShare met betrekking tot mail. Voor andere vormen van ad-hoc communicatie (vb. Whatsapp) zijn nog geen concrete afspraken gemaakt. Dergelijke afspraken zijn noodzakelijk om én éénduidige vorm van (formele en informele) communicatie te gebruiken én duidelijke richtlijnen op te stellen wanneer welke vorm van communicatie gehanteerd dient te worden.
Binnen het nieuw op te stellen informatiebeveiligingsbeleid (BIO-conform), zal hier aandacht aan worden besteed.

7. Verantwoording

Aanbevelingen:

1) Zorg te dragen dat in kader van audits en interne- en accountant controles vastlegging van procedurele zaken (aantoonbaarheid) een standaard wordt.

Ad 1) Algemeen doen we de zaken correct, alleen is dit richting de auditors en accountants veelal onvoldoende aantoonbaar. Daar in de AVG verantwoording (art. 5 lid 2) een belangrijk ‘nieuw’ gegeven is, dienen we aantoonbaarheid in de vorm van bewijslast te kunnen overleggen. Bij het niet aantoonbaar hebben van concrete bewijslast hoe we als SED organisatie of separate gemeente de privacy-zaken onder ‘controle’ hebben, kan dit een boete (of last onder dwangsom) opleveren van maximaal € 10.000.000,00. Ook in kader van het bewaken van de kwaliteit is dit een noodzakelijkheid. Dit betekent dat in de processen bewijslast/aantoonbaarheid opgenomen dient te worden.

8. Aanbevelingen

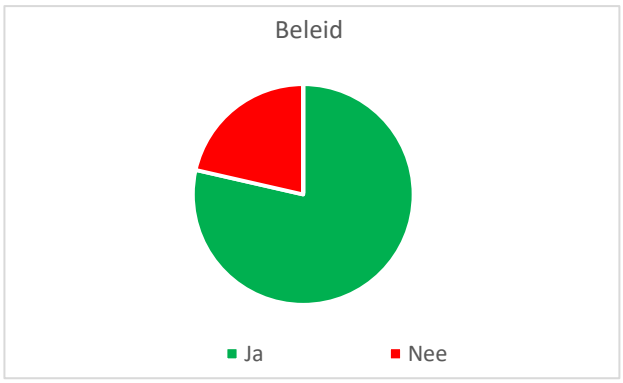
In deze rapportage worden een aantal aanbevelingen gedaan. Met de invulling van deze aanbevelingen zal de kwaliteit van de uitvoering van de privacy wetgeving worden verhoogd. Echter, iedere uitvoering van benoemde aanbevelingen kost tijd, menskracht en (hierdoor) geld en zal ten koste gaan van andere projecten en/of aanbevelingen.

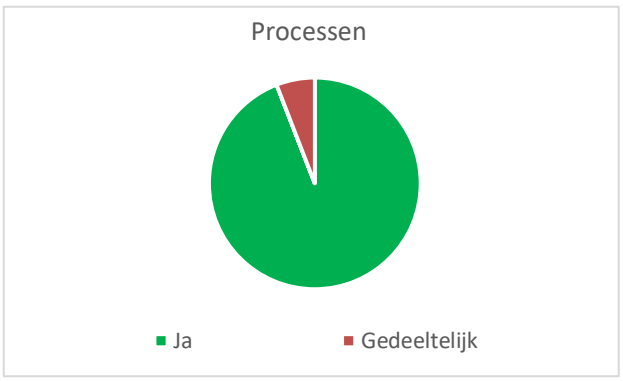
Als FG adviseer ik in kader van prioritering, de nadruk te leggen op onderstaande aanbevelingen:

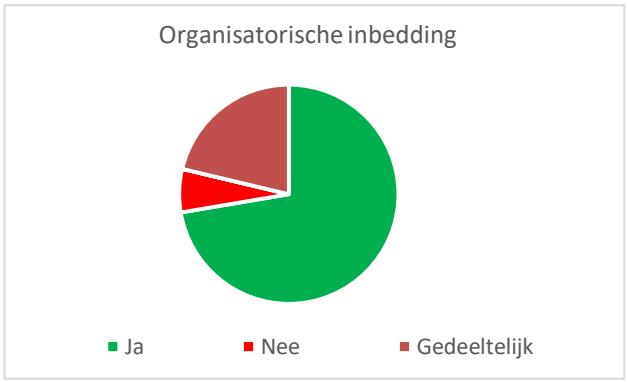
1) Processen vastleggen. Niet alleen de kwaliteit van de uitvoering van de privacy wetgeving zal hierdoor sterk verbeteren, omdat inzicht in gegevensstromen een essentieel onderdeel vormt, maar tevens omdat hier vele andere positieve effecten aan te ontleden zijn (vb. kosten, doorlooptijden, kwaliteit, etc.) Duidelijk mag zijn dat het vastleggen van meer dan 600 processen binnen het totale gemeentelijke domein een enorme klus is. Met betrekking tot privacy is het bepalen en vastleggen van kritische processen een goede start. Een gezamenlijk optrekken met AO/IB is hierin zeker denkbaar;

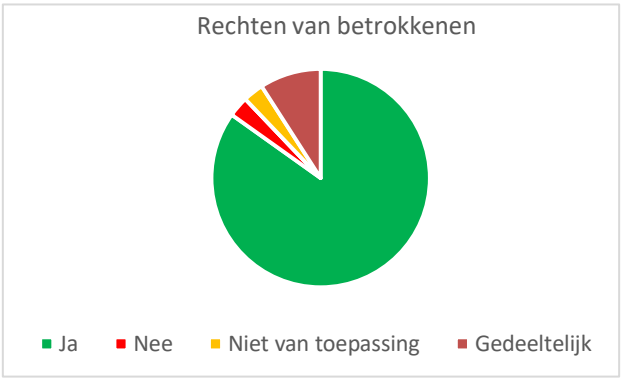
2) Het (her-)uitvoeren van DPIA's welke eind 2017 zijn uitgevoerd. De AVG stelt dat DPIA's periodiek getoetst dien te worden. Enerzijds biedt dit mogelijkheden om direct het onder punt 1 benoemde uit te voeren en anderzijds geeft het inzicht en verbetering in de risico-beheersing op het gebied van privacy en informatiebeveiliging. Ook hier betreft het in de eerste plaats DPIA's over de meest kritische processen (vb. processen rondom jeugd, WMO en OOV);
3) Directie en management meer te ondersteunen in de verantwoordelijkheid welke zij hebben op de uitvoering rondom de privacy en informatiebeveiliging. Enerzijds kan dit door de FG en CISO op reguliere basis uit te nodigen bij afdelingsoverleggen, anderzijds door periodiek de FG en CISO de status van beide onderwerpen toe te lichten in het directie- en managementoverleg. Ook een actieve informatievoorziening vanuit FG en CISO richting directie en management is hierin ondersteunend.

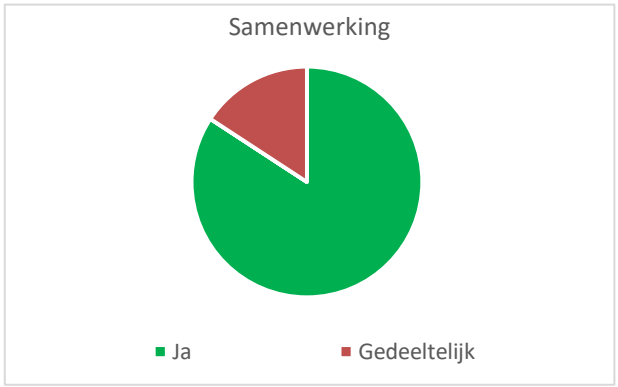
Bijlage 1. Stand van zaken AVG per onderwerp

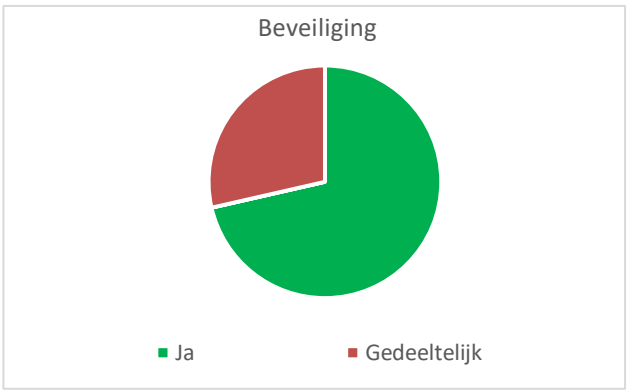


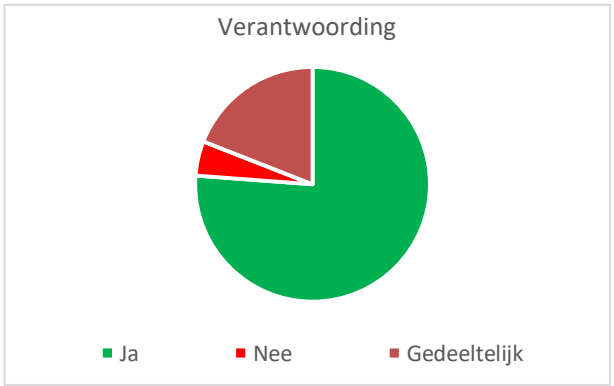


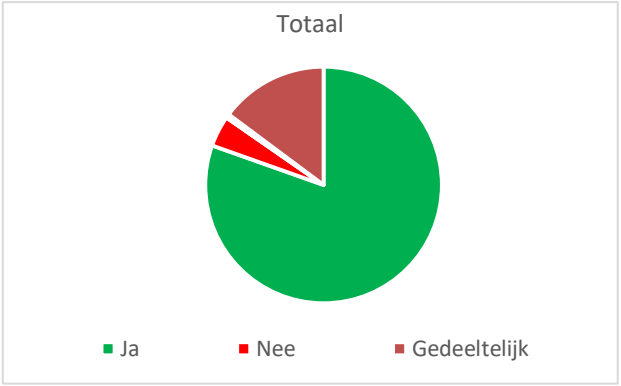












Bijlage 2. Uitgevoerde DPIA's vanaf medio 2019 – heden

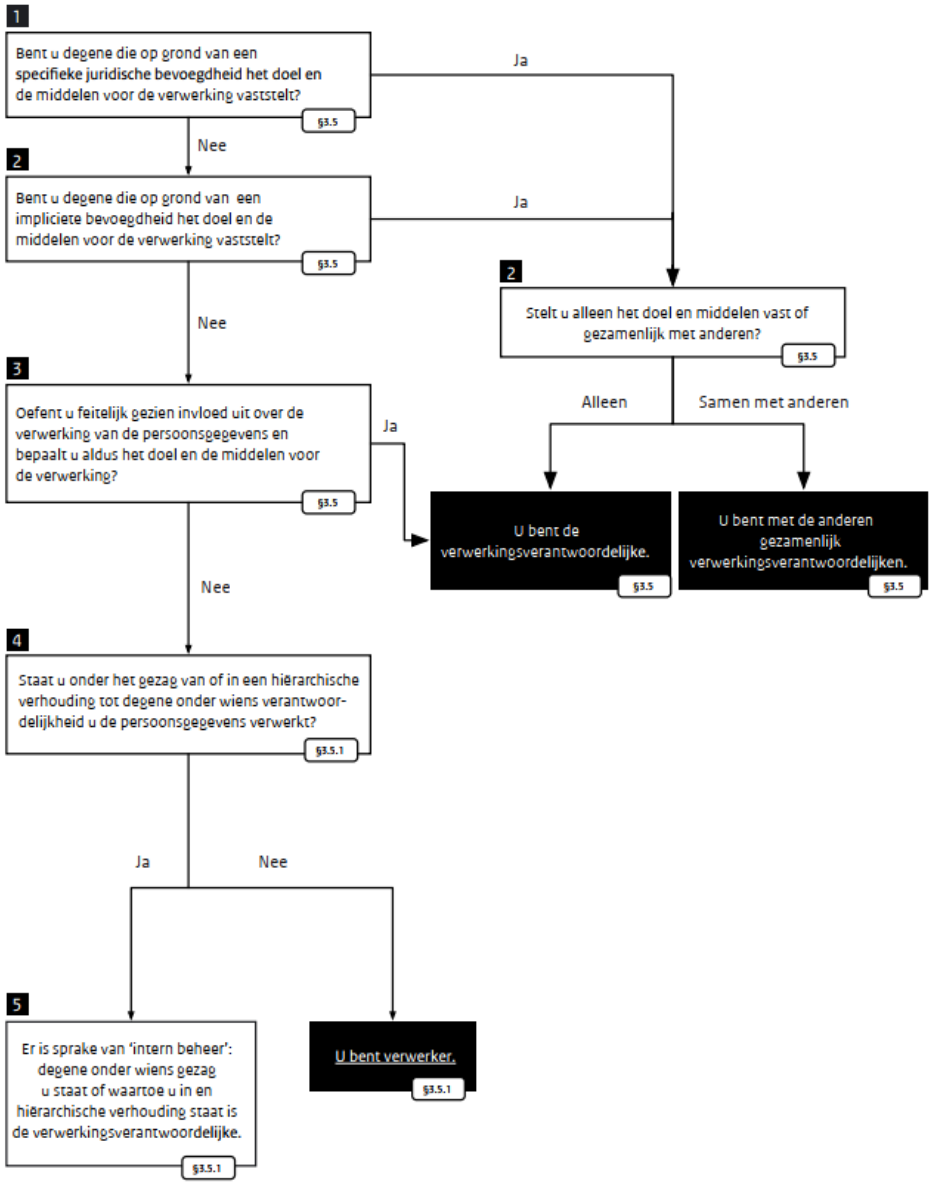
Voor SED:

- Kinderkledingbank
- Schuldhulpverlening (applicatie Allegro)
- Geo-uitwisseling

Regionaal:

- Scanstraat (totale proces)
- Uitvoering SaaS archivering (e-Depot)
- Intranet (IntraSED en gekoppeld systeem tussen rego-gemeenten)

Bijlage 3. Beslisboom verantwoordelijke/verwerker



Bijlage 4. Informatiebeveiligingsissues en datalekken

Informatiebeveiligingsincidenten van 1 juli 2019 tot en met 30 juni 2020

Informatie-incidenten zijn niet allen datalekken. Alle incidenten waar persoonsgegevens bij betrokken zijn, zowel in kader van het niet beschikbaar zijn en/of onjuistheden bevatten (integriteit), noemen we datalekken.

Datalekken dienen wel te allen tijde geregistreerd te worden, maar niet altijd aan de Autoriteit Persoonsgegevens (AP) gemeld te worden. Indien de mogelijkheid bestaat dat het datalek ernstige gevolgen kan hebben voor betrokkene(n) (te denken valt aan mogelijkheden als: identiteitsfraude, discriminatie, uitsluiting, nadelige financiële gevolgen of ernstige fysieke gevolgen), dan is een melding aan de AP geïndiceerd.

De AP kan een onderzoek doen naar het gemelde datalek. Indien verantwoordelijken een (ernstig) datalek niet melden, kan bij het toch bekend worden hiervan bij de AP, een onderzoek volgen. Uiteindelijk kan dit financiële gevolgen hebben voor de verantwoordelijk in de vorm van schadevergoeding aan betrokkene(n) en een mogelijke boete van de AP (maximaal voor datalekken: € 800.000,00 per incident). Daarnaast kan de AP een aanvullende boete opleggen aan de verantwoordelijke als blijkt dat het hier een structurele tekortkoming betreft in kader van informatiebeveiliging. Een boete kan betreffen: een straf onder dwangsom (tekortkoming oplossen binnen een door de AP gestelde termijn) of een boete op basis van de AVG, wat maximaal € 10.000.000,00 per incident kan betekenen.

Het is derhalve zaak om informatiebeveiligingsincidenten altijd te (laten) melden en een goede beoordeling te doen of er al dan niet gemeld moet worden aan de AP, betreffende een datalek.

Voor het registreren van beveiligingsincidenten gebruiken we momenteel (nog) excel. Alle meldingen welke ons gemeld worden, dan wel de meldingen welke ons bekend zijn, worden opgenomen in dit register. Onderstaande is verdeeld over het 2e half jaar 2019 (van 1 juli t/m 31 december) en het 1e half jaar 2020 (van 1 januari t/m 30 juni).

Informatiebeveiligingsincidenten : van 1 juli 2019 t/m 31 december 2019:

Bonfire (Locker-Goga Ransomeware) dreiging	Cyber-dreiging	4-7-2019	IBD/NCSC	Vertrouwelijkheid, beschikbaarheid en Integriteit	SSC DeSom actief op de hoogte gesteld van RansomeWare dreiging. OP bestaande C2-servers wordt gekeken naar mogelijke aanvallen en ADS-dumps.	Er zijn geen sporen aangetroffen, aldus SSC DeSom. Er staan momenteel geen C2 servers in het netwerk.	Nee	Nee
Verhoogd aantal Spear Phishing Mails	Phishing mails	26-7-2019	IBD	Vertrouwelijkheid, beschikbaarheid en Integriteit	Bericht op IntraSED geplaatst om bewust te zijn van dergelijke mail welke afkomstig lijken te zijn van hoog geplaatste functionarissen binnen een bedrijf, zoals de directeur, CIO, bussiness controler, etc.	Vooralsnog lijken er geen berichtgeving te zijn.	Nee	Nee
IBD beveiligingsadvies IBD-2019-0574 (H/H) betreffende kwetsbaarheden in VxWorks (besturingssysteem)	Cyber-dreiging	31-7-2019	IBD/NCSC	Vertrouwelijkheid, beschikbaarheid en Integriteit	Doorgezonden aan SSC DeSom.	Er wordt geen gebruik gemaakt van VxWorks besturingssystemen	Nee	Nee
brief verzonden aan verkeerd adres	Datalek	8-8-2019	Medewerker SD	Vertrouwelijkheid	Brief met (algemene) persoonsgevens verzonden aan verkeerd adres.	Melding opgenomen. Betreft geen hoog risico. Inwoner meldt dit zelf en heeft (geopende) brief afgegeven aan balie	Ja	Nee
Storing BRP-gegevens in Suwinet	Suwinet	8-8-2019	M. Muis/BKWI	Beschikbaarheid	Melding dat er een storing is bij de RViG (14:17) m.b.t. BRP-gegevens	Melding wordt doorgezet naar Suwinet-gebruikers	Nee	Nee
Storing BRP-gegevens in Suwinet (vervolg-melding)	Suwinet	8-8-2019	M. Muis/BKWI	Beschikbaarheid	Melding dat de storing bij de RViG (14:17) m.b.t. BRP-gegevens is opgelost (16:08)	Melding wordt doorgezet naar Suwinet-gebruikers	Nee	Nee
Onvoldoende beveiliging overheden/gemeenten	Cyber-dreiging	30-8-2019	IBD/VNG	Vertrouwelijkheid, beschikbaarheid en Integriteit	Informatie meenemen bij rapportages voor Colleges en Raden. Faalkaart geeft algemene tendensen en is a-specifiek.	Bewust te zijn/raken van algemene tendensen. Kan aanvulling zijn op Informatiebeveiliigngsbeleid en -plan. Informeren van directie SED en colleges blijft noodzakelijk op dit gebied.	Nee	Nee
Melding onderhoud werkzaamheden Suwinet	Suwinet	3-9-2019	M. Muis/BKWI	Beschikbaarheid	Ingeplande werkzaamheden Suwinet (03-09-2019 vanaf 18:00 uur)	Nieuwe release succesvol uitgevoerd. Suwinet weer beschikbaar (04-09-2019 vanaf 07:00 uur.	Nee	Nee
WMO beschikking naar verkeerde afzender gezonden	Datalek	4-9-2019	Medewerker SD	Vertrouwelijkheid	WMO beschikking is verzonden aan verkeerde afzender. Betrokkenen zijn geïnformeerd	Daat het informatie betreft met enige bijzondere persoonsgegevens is er een risico ingeschat waarbij een melding naar AP gerechtvaardigd is.	Ja	Ja
Brief verkeerd bezorgt (t.b.v. gemeente Medemblik)	Datalek	11-sep	DIV-afdeling	Vertrouwelijkheid	De post wordt centraal gescand en er is een brief verkeerd retour gezonden. Deze was bedoeld voor de gemeente Medemblik en is bezorgd aan de SED Organisatie	Brief wordt terug gezonden aan gemeente Medemblik.	Ja	Nee
Mail naar onjuist afzender	Datalek	13-9-2019	Medewerker SD	Vertrouwelijkheid	Mail met vraag over inkomsten-specificatie is naar onjuist mailadres gezonden. Hoewel persoonsgegevens gebruikt zijn (mailadres en achternaam) is de vraagstelling niet heel specifiek.	Gezien aard van datalek is er een nihil risico. Medewerker SD zal vragen te mail te vernietigen. Juiste klant is op de hoogte gesteld.	Ja	Nee
Kwestbaarheden in VPN's FortiGate	Cyber-dreiging	1-okt	IBD	Vertrouwelijkheid, beschikbaarheid en Integriteit	Doorgezonden aan SSC DeSom.	Er zijn/worden maatregelen ingezet door de Fortigate Firewall beheerder om deze kwestbaarheden te beperken/op te lossen. Er zijn geen redenen aan te nemen dat van deze kwestbaarheden misbruik is gemaakt.	Nee	Nee
Storing SVB-gegevens in Suwinet	Suwinet	23-10-2019	M. Muis/BKWI	Beschikbaarheid	De SVB-gegevens zijn niet zichtbaar binnen Suwinet (08:51)	Melding wordt doorgezet naar Suwinet-gebruikers	Nee	Nee
	Suwinet	23-10-2019	M. Muis/BKWI	Beschikbaarheid	De SVB-gegevens zijn wer zichtbaar binnen Suwinet (13:24)	Melding wordt doorgezet naar Suwinet-gebruikers	Nee	Nee
Problemen WIS-portaal (UWV-gegevens)	Suwinet	27-nov	M. Muis/BKWI	Beschikbaarheid	WIS-gegevens worden niet correct getoond. Na update van dit onderdeel blijkt dat de storing omtrent de WIS-gegevens nog niet is opgelost. Men stelt een nader onderzoek in	Wachten op uitsluitsel onderzoek. Medewerkers geïnformeerd	Nee	Nee
Melding onderhoud werkzaamheden Suwinet / WIS-gegevens UWV	Suwinet	28-11-2019	M. Muis/BKWI	Beschikbaarheid	Ingeplande werkzaamheden Suwinet (28-11-2019 vanaf 18:00 uur). Ook de WIS-gegevens (UWV) worden hierin meegenomen om tot een oplossing te komen.	Nieuwe release succesvol uitgevoerd. Suwinet weer beschikbaar (29-11-2019 vanaf 07:00 uur. Ook de WIS-gegevens worden weer vertoond.	Nee	Nee
Phishing-mail campagne / misbruik Belastingdienst	Phishing mails	4-dec	IBD	Vertrouwelijkheid, beschikbaarheid en Integriteit	Er doen zich veel phishing-mail meldingen voor binnen gemeenten betreffende zogenaamde Belastingdienst mailings. Wrs. Bedoeld inloggegevens buit te maken. Bericht geplaatst op IntraSED om hier op te attenderen.	Er zijn geen meldingen binnen gekomen van dergelijke mails.	Nee	Nee
Phishing-/fraude-mail - factuur domeinnaamregistratie	Fraude	12-12-2019	Bestuurssecretariaat	Integriteit	Op IntraSED melding gemaakt van dergelijke nep-facturen	Verder niets vernomen. Deze mail verwijderd.	Nee	Nee
Mail naar verkeerde afzender	Datalek	17-12-2019	Medewerker RO	Vertrouwelijkheid	Mail wordt verzonden naar verkeerd eafzender. Betreft een verwisseling van namen m.b.t. dezelfde (klacht-)melding omtrent verkeerssituatie. De betrokkenen is zeer boos en uit een klacht. FG belt terug en meldt situatie.	Hoewel er sprake is van een datalek zijn de betrokken persoonsgegevens zeer beperkt. Het risico is dan ook nihil. Betrokkenen is m.n. boos over onvoldoende informatie. Excuses hiervoor zijn aangeboden. Later volgt een klachtmelding van betrokkene, welke door afdelingshoofd wordt afgehandeld. Excuses zijn aangeboden	Ja	Nee
Zorggegevens verkeerd verzonden	Datalek	18-12-2019	Gem. Opmeer	Vertrouwelijkheid	Mail verzonden met bijlage welke per (regio-)gemeente geknipt had moeten worden m.b.t. de aanhangende bijlagen. Bijlagen betrof algemene en bijzondere persoonsgegevens van 15 betrokkenen binnen deze regio-gemeenten. Afzender betrof 2 (vaste) medewerkers van de SED organisatie.	Er is daarop volgende een verzoek uitgegeaan van de afzender om de bijlagen te verwijderen van de mail (in de mail stonden geen persoonsgegevens). Dit is gedaan en bevestigd aan de afzender (gemeente Opmeer). Gemeente Opmeer heeft het datalek gemeld aan AP. Aangezien er geen ernstige problemen voor de betrokkenen zullen onstaan is verdere actie (waaronder melding aan AP aan SED-zijde) niet nodig.	Ja	Ja (indirect)
Melding onderhoud werkzaamheden Suwinet	Suwinet	19-12-2019	M. Muis/BKWI	Beschikbaarheid	Ingeplande werkzaamheden Suwinet (19-12-2019 vanaf 18:00 uur).	Nieuwe release succesvol uitgevoerd. Suwinet weer beschikbaar (19-12-2019 vanaf 07:00 uur.	Nee	Nee
Kwestbaarheid binnen Citrix systemen	Cyber-dreiging	24-12-2019	IBD/NCSC	Vertrouwelijkheid, beschikbaarheid en Integriteit	Doorgezonden aan SSC DeSom. Binnen een half uur tijd wordt duidelijk dat het systemen betreft welke ook bij SSc DeSom draaien. Betreft de 'thuiswerk-module'.	Er zijn, door Citrix aanbevolen, mitigerende maatregelen doorgevoerd. Deze zijn rond 18:30 uur toegepast. SSC DeSom blijft monitoren op de Citrix-omgeving. Er zijn geen redenen aan te nemen dat eerder van deze kwestbaarheid misbruik is gemaakt.	Nee	Nee

INFORMATIE
BEVEILIGINGS
DIENST

Informatiebeveiligingsincidenten : van 1 januari 2020 t/m 30 juni 2020:

Kwetsbaarheid:	Betreft	Datum melding	Door:	BIV	Actie:	Resultaat:	Datalek	Melding AP	Opmerking
Problemen aanmelden Portal en diverse apps	Citrix en backoffice servers / Firewall probleem	13-1-2020	SSC DeSom	Beschikbaarheid	SSC DeSom reboot Firewall	Portal en BO-app werken weer. Pinautomaten 3 gemeenten (nog niet)	Nee	Nee	Later in de middag werken Pinautomaten weer
Citrix kwetsbaarheden op Netscaler	Citrix thuiswerkoplossing mogelijke kwetsbaarheid voor ongeoorloofde toegang en binnendringen in gemeentelijk netwerk	16-1-2020	IBD/NCSC	BIV (allen)	In overleg met SSC DeSom wordt de Citrix Netscaler down gezet.	Vanaf thuis inloggen is daarmee niet meer mogelijk. Het blijkt op dat moment ook meerdere applicatie te raken, waaronder de webmail functionateit en wat kleine communicatie-tools	Nee	Nee	
Citrix Netscaler down	Na.a.v. meldingen IBD/NCSC is als voorzorg de Citrix Netscaler in de DMZ uitgezet. Thuiswerken is niet mogelijk	17-1-2020	SSC DeSom	Beschikbaarheid	Citrix Netscaler is uit gezet. Aantal andere apps ondervinden problemen hierdoor	Thuiswerken niet mogelijk. Wachten op update van Citrix Netscaler om de kwetsbaarheid te dichten. Omdat mail ook hierdoor ook 'getroffen' is wordt een bypass gemaakt. Diverse andere (kleine) by-passes worden door SSC DeSom aangelegd. Ook wordt een sporenonderzoek gestart om te beoordelen of hackers binnen zijn geweest cq. pogingen daartoe hebben ondernomen.	Nee	Nee	Op vrijdag 24 is de patch vanuit Citrix ontvangen. Deze wordt zaterdag 25 januari geInstalleerd en getest. Maandag 27 januari wordt er meer bekend
Post verzonden aan verkeerde afzender	Datalek	4-2-2020	Medewerker DIV	Vertrouwelijkheid	Datalek gemeld. Specifiek aangegeven welke handelingen hiervoor verder nodig zijn	Geen hoog risico. Medewerker meldt excuses aan betrokkenen	Ja	Nee	
Diverse Covid-19 phishing-mails	Er gaan diverse mails rond omtrent thuiswerken met diverse (on-)mogelijkheden, waarbij via links deze mogelijkheden worden aangezet.	mrt-20	IBD/Media	BIV (allen)	Veel meldingen worden via IntraSED gecommuniceerd aan medewerkers	(Hopelijk) beperkte invloed op zakelijke informatie	Nee	Nee	Melding op IntraSED
Verkeer (beveiligde) mail verzonden aan verkeerde afzender	Datalek	apr-20	Medewerker SD	vertrouwelijkheid	Jeugdperspectiefplan is verzonden via beveiligde mail naar een aantal betrokkenen. Daarbij ook naar een verkeerde afzender incl. het daarbij behorende mobiele telefoonnummer (2FA). Hierdoor kon het plan geopend worden. Fout is ontdekt doordat de onjuist geadresseerde hiervan melding deed.	Er is gevraagde om de mail en bijlage te vernietigen. Daar het jeugd betreft en het plan (dus) is geopend is melding aan AP geïndiceerd. Betrokkenen zijn op de hoogte gesteld en excuses aangeboden. Risico lijkt vooralsnog nihil, vanwege melding onjuiste afzender.	Ja	Ja	6b64a79b-3d53-4f6e-b85a-819d03527a7c
Verkeerde bijlage in brief	Datalek	apr-20	Medewerker SD	Vertrouwelijkheid	Datalek gemeld. Bijlage betrof 2 specificaties minima-gegevens. Eén voor de juiste klant, een ander voor een andere inwoner.	Geen hoog risico. Klant meldt zich bij balie om de verkeerde bijlage af te geven. Medewerker SD meldt excuses aan betrokkenen	Ja	Nee	
Traagheid Citrix	Citrix via portal verloppt momenteel erg traag	apr-20	SSC DeSom/SED medewerkers	Beschikbaarheid	Citrix is traag, hierdoor alle apps traag. Is gemeld bij SSC DeSom.	SSC DeSom zal hedenavond actie ondernemen	Nee	Nee	
Aankondiging Suwinet onderhoud	Suwinet onderhoud / sommige functionaliteit niet beschikbaar	17-4-2020	BKWI	Beschikbaarheid	n.v.t.	n.v.t.	Nee	Nee	
Diverse spookfacturen	Spookfacturen	21-4-2020	Medewerker(s)	Vertrouwelijkheid en integriteit	Er worden een aantal meldingen doorgegeven van spookfacturen. Met name domeinnaamregistraties. Kleine bedragen	Er wordt via IntraSED gewaarschuwd tegen deze spookfacturen en aangegeven eerst, bij twijfel, te overleggen	Nee	Nee	Melding op IntraSED
Storing WKBI: niet mogelijk om de inkomstengegevens op te vragen.	Suwinet storing	1-5-2020	BKWI	Beschikbaarheid	n.v.t.	n.v.t.	Nee	Nee	
Uittreksel GBA naar verkeerd adres gezonden	Datalek: verkeerd postadres	1-5-2020	Medewerker GBA	Vertrouwelijkheid	Excuses aangeboden aan beide personen. Gevraagd document te vernietigen	Datalek wordt als zeer beperkt risico gezteld, mede doordat verkeerd gedresseerde zelf melding heetf gemaakt en brief heeft vernietigd	Nee	Nee	
Gebruik van videoconferencin-tools	Welke video-conferencing-tool is veilig (privacy-technische)	1-5-2020	IM-team	Vertrouwelijkheid	Staatje gemaakt met voor- en nadelen van diverse tools.	Momenteel is MS-teams de meest handige tool, omdat iedere interne medewerker het heeft en de informatie-opslag past binnen het beleid.	Nee	Nee	
Problemen alarm Stadskantoor Enkhuizen	Alarm staat nietcorrect ingesteld. Veel 'valse' meldingen	12-5-2020	SED Servicedesk	BIV (allen)	Controle alarminstallatie en leverancier ingeseind. Aanpassingen gedaan	Alarmering getest.	Nee	Nee	
Post verzonden aan verkeerde afzender	Datalek	18-5-2020	Medewerker SD	Vertrouwelijkheid	Datalek gemeld.	Geen hoog risico. Medewerker meldt excuses aan betrokkenen	Ja	Nee	
Datalek gegevens FIXI-app	Informatie FIXI-app breed inzichtelijk	25-5-2020	Inwoner Enkhuizen	Vertrouwelijkheid	FIXI_app app meldingen openbare ruimten) toont meldingen van inwoners met pers. Gegevens	datalek, gemeld aan leverancier en AP.	Ja	Ja	17fcee71-4289-489e-9c2d-40fa389f5b46
Bevraag-services Suwinet 'out of order'	Tijdelijke buiten dienst i.v.m. onderhoud	27-5-2020	BKWI	Beschikbaarheid	Mededelen aan Suwinet medewerkers	N.v.t.	Nee	Nee	
Probleem: storing Oracle	Aantal bedrijfskritische apps werken niet	8-6-2020	SSC DeSom	Beschikbaarheid	SSC DeSom pakt dit met hoogste prio (1) op.	Na ca. 1 uur is het probleem opgelost. Apops werken weer	Nee	Nee	
Onderhoud Suwinet	Suwinet	12-6-2020	BKWI	Beschikbaarheid	Mededelen aan Suwinet medewerkers	N.v.t.	Nee	Nee	
Problemen bevragen van GBA/BRP berichten	Suwinet	12-6-2020	BKWI	Beschikbaarheid	Mededelen aan Suwinet medewerkers	N.v.t.	Nee	Nee	
Onderhoud switches (ring) leverancier bij SSC DeSom	SSC DeSom / ingepland onderhoud	26-6-2020	SSC DeSom / leverancier	Beschikbaarheid	Hierdoor vervalt verbindingen met alle locaties. Werken is niet mogelijk vanuit netwerk en WiFi. Thuiswerken is wel mogelijk	Valt onder regulier netwerk onderhoud en gebeurd standaard in de late middag- en avonduren	Nee	Nee	