Jaarrapportage informatieveiligheid en privacy 2019
Gemeente Waterland

Gemeente Waterland

Inhoud

1. Inleiding

De gemeente streeft naar continue en betrouwbare dienstverlening, het zorgvuldig omgaan met informatie en het beheersen van risico's. Met de ambitie te voldoen aan de Baseline Informatiebeveiliging Gemeenten (BIG), hét gemeentelijke basisnormenkader voor informatieveiligheid en wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG).

Deze rapportage geeft op hoofdlijnen de uitkomsten weer van de gemeente-brede uitgevoerde zelfevaluatie informatieveiligheid over het jaar 2019. Deze zelfevaluatie is gebaseerd op de BIG en is uitgevoerd in de periode juli t/m december 2019. Wij rapporteren als gemeente Waterland op één moment in het jaar over de status van onze informatieveiligheid. De methodiek daarvoor is de 'Eenduidige Normatiek Single Information Audit' (ENSIA). Via ENSIA wordt verticaal verantwoording afgelegd aan de toezichthouders van de rijksoverheid en horizontaal aan de gemeenteraad. Voor de verantwoording aan de gemeenteraad sluit ENSIA middels deze jaarrapportage aan op de gemeentelijke P&C-cyclus als onderdeel (bijlage) van de Jaarrekening.

Verantwoording wordt afgelegd over de Basisregistratie Personen (BRP), de wetgeving voor Reisdocumenten (Paspoortuitvoeringsregeling Nederland/PUN), de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT), de Basisregistratie Ondergrond (BRO), Digitale persoonsidentificatie (DigiD) en de Gezamenlijke elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet). Daarnaast wordt de status van informatieveiligheid in brede zin conform de BIG verantwoord en de status van maatregelen en verplichtingen op grond van de AVG.

In verband met het openbare karakter van de rapportage is geen detailinformatie opgenomen.

Van Big naar BIO

Voor de verslaglegging is deze rapportage nog opgesteld conform de BIG en BIG hoofdstukindeling. Vanaf 2020 werken wij als overheid op basis van de Baseline Informatiebeveiliging Overheid, de BIO. Waar van toepassing zijn verbetermaatregelen uit de zelfevaluatie vertaald naar deze nieuwe baseline.

IT audit over DigiD en Suwinet

Voor 2019 geldt dat de verantwoording over DigiD en Suwinet aan de stelselhouders BZK/Logius en het ministerie SZW wordt verantwoord door middel van een Collegeverklaring. Deze Collegeverklaring is opgesteld op basis van de bevindingen uit de zelfevaluatie en onderbouwende bewijsstukken. De Collegeverklaring is getoetst door een onafhankelijke IT auditor. Deze neemt de bevindingen op in een assurancerapport. Met de vastgestelde Collegeverklaring en het assurancerapport voldoen wij aan de verantwoordingsplicht voor DigiD en Suwinet. De uitkomsten uit de zelfevaluatie zijn op hoofdlijnen in deze rapportage opgenomen (hoofdstuk 3). De tekst van de Collegeverklaring treft u aan in bijlage 1.

Bestuurlijke verantwoording over de BAG, BGT en BRO

Voor de BAG, BGT en BRO zijn over 2019 separate zelfevaluaties in ENSIA uitgevoerd. De domein specifieke verantwoordingsrapportages BAG, BGT en BRO zijn als bijlage bij deze jaarrapportage opgenomen. De scores zijn opgenomen in de samenvatting resultaten zelfevaluatie 2019 (hoofdstuk 2).

2. Samenvatting resultaten zelfevaluatie 2019

Zelfevaluatie	Norm	Gemeente Waterland
DigiD (IT audit)	100%	100%
Suwinet (IT audit)	100%	100%
BRP domeinvragen Kwaliteitsmonitor RvIG BRP informatiebeveiligingsvragen ENSIA Samengevoegd resultaat	 90%	669 punten van 800 (83,6%) 1.127 punten van 1.200 (93,9%) 1.796 punten van 2.000 (89,8%)
Reisdocumenten domeinvragen Kwaliteitsmonitor RvIG Reisdocumenten informatiebeveiligingsvragen ENSIA Samengevoegd resultaat	 90%	1.243 punten van 1.400 (88,7%) 584 punten van 600 (97,3%) 1.827 punten van 2.000 (91,3%)
BAG	75%	83%
BGT	75%	60%
BRO	60%	54,2%
BIG (hoofdstuk) – Maatregelen:		
BIG (h3) - implementatie van de Tactische Baseline	-	grotendeels aan voldaan
BIG (h4) - gemeentelijke samenwerking (VERVALLEN)	-	-
BIG (h5) - beveiligingsbeleid	-	voldaan
BIG (h6) - organisatie van de informatiebeveiliging	-	grotendeels aan voldaan
BIG (h7) - beheer van bedrijfsmiddelen	-	grotendeels aan voldaan
BIG (h8) - personele beveiliging	-	grotendeels aan voldaan
BIG (h9) - fysieke beveiliging en beveiliging van de omgeving	-	voldaan
BIG (h10) - beheer communicatie- en bedieningsprocessen	-	grotendeels aan voldaan
BIG (h11) - toegangsbeveiliging	-	grotendeels aan voldaan
BIG (h12) - verwerving, ontwikkeling en onderhoud van informatiesystemen	-	grotendeels aan voldaan
BIG (h13) - beheer van informatiebeveiligingsincidenten	-	voldaan
BIG (h14) - bedrijfscontinuïteitsbeheer	-	grotendeels aan voldaan
BIG (h15) - naleving	-	voldaan

3. Uitkomsten IT audit DigiD en Suwinet

3.1. DigiD

DigiD is het authenticatiemiddel voor onze online dienstverlening. Het object van onderzoek was de webomgeving van DigiD aansluiting 999913 Digitaal Loket gemeente Waterland. De verantwoording aan de stelselhouder BZK/Logius vindt plaats door middel van de Collegeverklaring. Deze omvat het op 31 december 2019 in opzet en bestaan voldoen van de beheersmaatregelen aan de geselecteerde normen inzake DigiD. De beheersingsmaatregelen die zijn uitbesteed vallen buiten de reikwijdte van de Collegeverklaring. De Collegeverklaring en de verantwoording van de dienstverlener dekken tezamen alle geselecteerde normen inzake DigiD af.

Bevindingen

Voor DigiD aansluitnummer 999913 wordt door gemeente Waterland aan alle geselecteerde normen voldaan.

Uit de verantwoording van de dienstverlener bleek dat ook voor de beheersingsmaatregelen die zijn uitbesteed aan alle normen wordt voldaan.

3.2. Suwinet

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. De gemeente Waterland maakt gebruik van Suwinet voor de uitvoering van de Participatiewet, IOAZ en IOAW. Daarnaast maakt de gemeente gebruik van Suwinet voor niet Suwi-taken. Dit betreft Suwinet/Burgerzaken voor adresonderzoek. De verantwoording aan stelselhouder ministerie SZW vindt plaats door middel van de Collegeverklaring. Inzake Suwinet heeft de Collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan GR-BVO Halte Werk (Zelfstandigenloket). De Collegeverklaring omvat het op 31 december 2019 in opzet en bestaan voldoen van de beheersmaatregelen aan de geselecteerde normen inzake Suwinet.

Bevindingen

Voor de Suwinet-taken voldoen de interne beheersingsmaatregelen in opzet en bestaan aan alle geselecteerde normen inzake Suwinet.
Voor de niet Suwi-taken (Suwinet/Burgerzaken) werd op het moment van toetsing aan één norm niet geheel voldaan. Hiervoor is een verbeterplan opgesteld, dat in januari 2020 is uitgevoerd en afgehandeld, waarmee aan de norm wordt voldaan.

3.3. Collegeverklaring DigiD en Suwinet en assurancerapport IT auditor

De onafhankelijke IT auditor heeft op basis van de Collegeverklaring een voorlopig assurancerapport afgegeven. Naar oordeel van de IT auditor is de Collegeverklaring ENSIA 2019 inzake informatiebeveiliging van DigiD en Suwinet in alle van materieel belang zijnde aspecten juist. De Collegeverklaring informatiebeveiliging DigiD en Suwinet is vastgesteld op 7 april 2020, waarna de definitieve assurance van de IT auditor volgt. De tekst van de Collegeverklaring treft u aan in bijlage 1.

4. Uitkomsten BRP en Reisdocumenten

4.1. Inleiding

Het resultaat van de toetsing BRP en Reisdocumenten werd vorig jaar bepaald door samenvoeging van de resultaten van de ENSIA-verantwoording informatieveiligheid en de resultaten van de domein specifieke zelfevaluatie via de 'Kwaliteitsmonitor' van de Rijksdienst voor Identiteitsgegevens (RvIG). De totaalnorm werd daarbij gesteld op 90 %. Over 2019 is de zelfevaluatie gescheiden uitgevoerd. De informatiebeveiligingsvragen BRP en Reisdocumenten via ENSIA en de domeinvragen BRP en Reisdocumenten via de Kwaliteitsmonitor van de RvIG. De resultaten worden verstrekt in de vorm van uittreksels en zijn weergegeven in een puntenaantal.

De managementrapportages en uittreksels BRP en Reisdocumenten zijn in februari 2020 separaat voorgelegd aan het college van burgemeester en wethouders voor de verantwoording aan de stelselhouders. Een aantal actiepunten en aanbevelingen die in de managementrapportages zijn benoemd worden opgevolgd. In een enkel geval wordt van een maatregel of aanbeveling die geen risico vormt bewust en beargumenteerd afgeweken.

4.2. BRP

De normering die is gekoppeld schets een beeld van de toepassing van technische en organisatorische beveiligingsmaatregelen en overige aspecten van processen rondom de BRP. Uit de zelfevaluaties blijkt dat de gemeente Waterland voldoende scoort op de inrichting, de werking en de beveiliging van de basisregistratie.
Het samengevoegd resultaat van de domeinvragen en informatiebeveiligingsvragen is 1.796 punten van de maximaal 2.000 punten. Dat geeft een percentage van 89,8% voor zowel de wettelijke eisen als de aanbevelingen. Voor alleen de wettelijke eisen scoort de gemeente Waterland ruim 91%.

4.3. Reisdocumenten

De normering die is gekoppeld schets een beeld van de toepassing van technische en organisatorische beveiligingsmaatregelen en overige aspecten van het aanvraag- en uitgifteproces paspoorten en NIK. Uit de zelfevaluatie blijkt dat de gemeente Waterland goed scoort op de beveiliging en overige aspecten van het aanvraag- en uitgifteproces.
Het samengevoegd resultaat van de domeinvragen en informatiebeveiligingsvragen is 1.827 punten van de maximaal 2.000 punten. Dat geeft een percentage van 91,3%.

5. Status BIG

In dit hoofdstuk is een uitwerking per onderdeel uit de ENSIA zelfevaluatie opgenomen. De vragenlijst informatiebeveiliging BIG betreft de BIG-maatregelen voor informatieveiligheid in brede zin, zowel de fysieke- als logische beveiliging, en maatregelen ten aanzien van de Algemene Verordening Gegevensbescherming (AVG). De beantwoording, die is onderbouwd met bewijsstukken, geeft aan of wel of niet aan de maatregelen wordt voldaan, maar leidt niet tot een score. De ruim 170 vragen over de BIG-maatregelen zijn verdeeld over een aantal hoofdstukken, die in de paragrafen zijn opgenomen. Waar van toepassing is een verwijzing opgenomen naar de Baseline Informatiebeveiliging Overheid (BIO), die met ingang van 2020 van kracht is.

5.1. BIG hoofdstuk 3: Implementatie van de Tactische Baseline

Er zijn normen gesteld aan de wijze waarop de BIG is geïmplementeerd in de gemeentelijke organisatie. Dit is vertaald naar het benoemen van verantwoordelijken, het uitvoeren van een Baseline toets BIG, samenstellen van een implementatieplan en rapporteren over de voortgang van de informatiebeveiliging.

Bevindingen

Aan deze normen is grotendeels voldaan.

Tekortkoming

De gemeente beschikt over een Information Security Management Systeem (ISMS), maar deze is nog niet geheel ingericht met Plan-Do-Check-Act maatregelen voor gebruik in de organisatie.

Verbetermaatregel

Maatregelen worden nu gedurende de jaarlijkse ENSIA-verantwoording uitgezet en bewaakt. Het ISMS wordt ingericht zodra hiervoor capaciteit beschikbaar is.

5.2. BIG hoofdstuk 4: Risicobeoordeling bij gemeentelijke samenwerking (vervallen)

De vragen over risicobeoordeling bij gemeentelijke samenwerking zijn voor een deel bij andere BIG-hoofdstukken ondergebracht. Voor de verantwoording over 2019 is dit hoofdstuk komen te vervallen.

5.3. BIG hoofdstuk 5: Beveiligingsbeleid

Doelstelling is het aantoonbaar realiseren van een niveau van informatiebeveiliging op basis van relevante wetgeving. Als fundament voor het leveren van betrouwbare dienstverlening en het door kunnen gaan van kritische processen bij een calamiteit of incident. Het informatiebeveiligingsbeleid moet periodiek worden beoordeeld. Dit betreft voor de gemeente Waterland het informatiebeveiligingsbeleid, het Handboek beveiliging Suwinet, de procedures BRP en Reisdocumenten en het Privacy beleid. Deze zijn actueel, jonger dan 3 jaar en vastgesteld.

Bevindingen

Aan deze normen is voldaan.

5.4. BIG hoofdstuk 6: Organisatie van de informatiebeveiliging

Een adequate organisatie van informatiebeveiliging is vereist, waarbij de verantwoordelijkheden, functies en rollen zijn belegd, worden gemonitord en geactualiseerd. Medewerkers worden conform een autorisatieprocedure voor systemen, rollen en rechten geautoriseerd. Voor aanstelling wordt een VOG overlegd en een geheimhoudingsverklaring getekend. Met externe partijen worden vereiste beveiligingsmaatregelen opgenomen in een (verwerkers)overeenkomst. Het college van burgemeester en wethouders en het management zijn betrokken bij de beveiliging en over de voortgang van informatiebeveiliging en eventuele beveiligingsincidenten wordt gerapporteerd. De gemeente onderhoudt contacten met relevante (overheids)organisaties en expertisegroepen.

Bevindingen

Aan deze normen is grotendeels voldaan.

Tekortkoming

Het uitvoeren van een Data Protection Impact Assessment, (D)PIA, is verplicht voorafgaand aan nieuwe verwerkingen van persoonsgegevens waarbij sprake is van een verhoogd risico. De gemeente heeft nog geen (D)PIA uitgevoerd.

Verbetermaatregel

Met een externe partij zijn afspraken gemaakt om in 2020 door een Data Protection Officer in opleiding als werkopdracht een (D)PIA uit te laten voeren. Gestart wordt met het zaakgericht werken in de eSuite.

5.5. BIG hoofdstuk 7: Beheer van bedrijfsmiddelen

De bedrijfsmiddelen zijn actueel geregistreerd en er zijn regels voor een juist gebruik van ICT-middelen om de bedrijfsmiddelen adequaat te beschermen. De risico's en maatregelen zijn geclassificeerd. Op basis van een actuele 'ICT-foto' wordt de gemeente naast algemene meldingen gericht geïnformeerd over mogelijke kwetsbaarheden door de Informatiebeveiligingsdienst voor gemeenten (IBD). Verwerkingen die onder de verantwoordelijkheid van de gemeente plaatsvinden zijn en worden conform de AVG opgenomen in het 'Register van Verwerkingen'. In het register worden onder andere de verwerkingsactiviteiten, doeleinden van de verwerking, wettelijke grondslag, soort persoonsgegevens, met wie de gegevens eventueel worden gedeeld en de bewaartermijn van verwerkingen vermeld. Het register is nog in opbouw en bevat op dit moment 113 verwerkingen.

Bevindingen

Aan deze normen is grotendeels voldaan.

Tekortkoming

Alle informatiesystemen/processen behoren een verantwoordelijke (proces)eigenaar te hebben. Hoewel veel systemen/processen een (proces)eigenaar hebben, zijn deze nog niet formeel vastgesteld.

Verbetermaatregel

In 2020 worden de (proces)eigenaren formeel vastgesteld. Dit is conform de BIO maatregelen (BIO Control 8.1.2).

5.6. BIG hoofdstuk 8: Personele beveiliging

Doelstelling is het bewerkstelligen dat medewerkers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, geschikt zijn voor hun rollen en om risico's van diefstal, fraude of misbruik van faciliteiten te verminderen. Verantwoordelijkheden, rollen en rechten zijn vastgelegd. Voor aanstelling wordt de achtergrond van kandidaten onderzocht, een VOG opgevraagd en een geheimhoudingsverklaring getekend.

Bevindingen

Aan deze normen is grotendeels voldaan.

Tekortkomingen

De BIO stelt dat de directie van alle medewerkers en contractanten behoort te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie (BIO Control 7.2.1). Gedurende het dienstverband wordt het achtergrondonderzoek en/of overleggen van een VOG echter niet periodiek herhaald.
Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging (BIO Control 7.2.3). De gemeente Waterland heeft geen specifiek disciplinair proces (sanctiebeleid), maar past bij inbreuken op het informatiebeveiligingsbeleid waar nodig de CAR/UWO toe.

Verbetermaatregelen

Voor het periodiek herhalen van achtergrondonderzoeken wordt nog geen aanleiding gezien en wordt bewust van de norm afgeweken.
Er wordt een disciplinaire procedure opgesteld, met in begrip van het toepassen van de CAR/UWO bij inbreuken op de informatiebeveiliging. De procedure moet aansluiten op het Privacy beleid en integriteitsbeleid van de gemeente.

5.7. BIG hoofdstuk 9: Fysieke beveiliging en beveiliging van de omgeving

Doelstelling is het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein, ruimten, apparatuur en de informatie van de organisatie.

Bevindingen

Aan deze normen is voldaan.

5.8. BIG hoofdstuk 10: Beheer van communicatie- en bedieningsprocessen

Doelstelling is het waarborgen van een correcte en veilige bediening van ICT-voorzieningen. Taken en verantwoordelijkheden voor gebruik en beheer zijn gescheiden belegd. Bedieningsprocedures zijn beschreven en er is een vastgestelde procedure voor wijzigingenbeheer op ICT-voorzieningen voor het beheerst uitvoeren van wijzigingen, inclusief de scheiding van ontwikkeling, testen, acceptatie en productie (OTAP).

Bevindingen

Aan deze normen is grotendeels voldaan.

Tekortkoming

Als dienstverleners/leveranciers hun dienstverlening wijzigen voor processen/systemen die het primaire proces ondersteunen wordt niet altijd een risicobeoordeling uitgevoerd (BIO Control 15.2.2). In de meeste gevallen en vooral voor de kritische processen worden wijzigingen eerst getest in een testomgeving en gaan pas naar de productieomgeving na acceptatie van de gebruiker(s). Risicobeoordeling wordt gedaan, maar is nog niet structureel verankerd.

Verbetermaatregel

Risicobeoordeling als vast onderdeel meenemen en borgen in de test- en acceptatieomgeving.

5.9. BIG hoofdstuk 11: Toegangsbeveiliging

Doelstelling is het beheersen van de toegang tot informatie, op de werkplek als ook bij het werken op afstand. Toegangsrechten, autorisatie- en inlogprocedures, authenticatie, time-outsessies/clear screen zijn goed ingericht en actueel vastgesteld. De procedures en de juiste toekenning van rollen en rechten wordt stelselmatig gecontroleerd.

Bevindingen

Aan deze normen is grotendeels voldaan.

Tekortkoming

Medewerkers zijn geïnformeerd over het veilig omgaan met wachtwoorden, maar het bewustzijn op specifiek dit punt structureel herhalen is nog niet geborgd.

Verbetermaatregel

Dit onderdeel is meegenomen in de organisatie brede ‘presentatie informatiebeveiliging en privacy’ die zijn gestart in januari 2020. Deze presentatie wordt periodiek geactualiseerd en herhaald.

5.10. BIG hoofdstuk 12: Verwerving, ontwikkeling en onderhoud van informatiesystemen

Doelstelling is het bewerkstelligen dat beveiliging integraal deel uitmaakt van de gemeentelijke informatiesystemen. Bij het testen van software wordt gebruik gemaakt van geanonimiseerde testdata. Voor de beheersing van en regelmatige controle op technische kwetsbaarheden zijn maatregelen getroffen. Bij nieuwe of (sterk) gewijzigde processen/systemen is er aandacht voor informatiebeveiligingseisen en het voldoen aan de AVG. Als daarbij persoonsgegevens worden verwerkt is het uitvoeren van een Data Protection Impact Assessment, (D)PIA) verplicht. De BIO stelt dat voor het ontwikkelen van software en systemen regels behoren te worden vastgesteld en op ontwikkelingsactiviteiten binnen de organisatiemoeten worden toegepast (BIO Control 14.2.1). De gemeente Waterland ontwikkelt zelf geen software en heeft daarom geen beleid of richtlijnen daarvoor opgesteld. Hiervoor is dan ook geen verbetermaatregel opgenomen.

Bevindingen

Aan deze normen is grotendeels voldaan.

Tekortkoming

Er is nog geen standaardprocedure voor het uitvoeren van een (D)PIA.

Verbetermaatregel

In 2020 wordt een eerste (D)PIA uitgevoerd (zie hoofdstuk 6). Met de kennis die daarmee wordt opgedaan wordt een standaardprocedure voor het uitvoeren van een (D)PIA opgesteld.

5.11. BIG hoofdstuk 13: Beheer van informatiebeveiligingsincidenten

Doelstelling is het bewerkstelligen dat informatiebeveiligingsincidenten en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen. De gemeente Waterland heeft een incidentmanagementprocedure, registreert mogelijke kwetsbaarheden en incidenten en verzamelt bewijsmateriaal. De Informatiebeveiligingsdienst voor gemeenten (IBD) informeert de gemeente gericht over mogelijke kwetsbaarheden en incidenten. Het aantal en soort meldingen van (mogelijke) beveiligingsincidenten over 2019 is opgenomen in hoofdstuk 7.

Bevindingen

Aan deze normen is voldaan.

5.12. BIG hoofdstuk 14: Bedrijfscontinuïteitsbeheer

Doelstelling is het tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen en om tijdig herstel te bewerkstelligen. Er zijn risicoanalyses uitgevoerd en voor alle kritische processen is er een calamiteiten- en continuïteitsplan, waarin aandacht is besteed aan de continuïteit bij uitval en een uitwijkdraaiboek BRP.

Bevindingen

Aan deze normen is grotendeels voldaan.

Tekortkoming

Eén maatregel betreft het uitvoeren van een Business Impact Analyse (BIA), die de afhankelijkheid van processen en diensten van de ICT in kaart brengt. Deze is nog niet voor alle processen uitgevoerd.

Verbetermaatregel

In 2020 wordt dit meegenomen als onderdeel van de BIO (BIO Control 17.1.2) bij de verdere inrichting van het team Informatievoorziening.

5.13. BIG hoofdstuk 15: Naleving

Doelstelling is het voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen en van enige beveiligingseisen.

Bevindingen

Aan deze normen is voldaan.

6. Algemene Verordening Gegevensbescherming (AVG)

Voor de datum van inwerkingtreding van de AVG (25 mei 2018) had de gemeente Waterland al een proces ingericht in het kader van de Meldplicht Datalekken en een Functionaris Gegevensbescherming (FG) aangesteld.

In 2019 heeft de gemeente Waterland haar Privacy beleid vastgesteld en gepubliceerd op Mijn Overheid.
Op de website is een digitaal formulier geplaatst waarmee inwoners verzoeken in kunnen dienen over de verwerking van hun persoonsgegevens. Het formulier is gekoppeld aan DigiD om conform de AVG de identiteit van de verzoeker vast te kunnen stellen.

Voor bewustwording over beveiliging en privacy is organisatiebreed een online Digi-scan uitgezet, waar vragen over digitale veiligheid deel van uit maakten. De uitkomsten zijn meegenomen in de presentatie ‘Informatiebeveiliging en privacy’ die in januari 2020 start.

Over de status van maatregelen en verplichtingen van de AVG zijn vragen opgenomen in de ENSIA verantwoording zelfevaluatie BIG (zie hoofdstuk 5).

7. Incidenten

Een dreiging of tekortkoming in de beveiliging kan leiden tot een beveiligingsincident, een daadwerkelijke inbreuk op de beveiliging. Als daarbij persoonsgegevens zijn betrokken is er sprake van datalekken. Het is van groot belang dat (mogelijke) incidenten snel, adequaat gedetecteerd, gemeld en behandeld worden om de mogelijke nadelige gevolgen te voorkomen of te beperken. De gemeente Waterland heeft een procedure voor het melden van mogelijke incidenten en wordt specifiek en gericht geïnformeerd over kwetsbaarheden en incidenten door de IBD.

Meldingen 2019

In 2019 zijn 13 meldingen van mogelijke beveiligingsincidenten/datalekken ontvangen en opgenomen in het meldingenregister:

- 2 meldingen van CEO-fraude (phishing voor financieel gewin). Daar is adequaat op gereageerd zonder nadelige gevolgen. De fraudepoging is ter informatie gemeld aan de IBD en Fraudehelpdesk;
- 6 meldingen van (technische) kwetsbaarheden waarvan 1 niet van toepassing bleek en 5 snel en adequaat zijn opgelost. Er zijn geen nadelige gevolgen van ondervonden;
- 5 meldingen van een incident waarbij persoonsgegevens waren betrokken. Na onderzoek bleken drie incidenten daadwerkelijk datalekken die zijn gemeld aan de Autoriteit Persoonsgegevens en in twee gevallen ook aan de betrokkenen. De incidenten (twee extern en één intern veroorzaakt door een menselijke fout) zijn direct in behandeling genomen en hersteld.

Bijlage 1: Tekst Collegeverklaring ENSIA 2019

Vanwege het openbare karakter van deze jaarrapportage is alleen de tekst van de Collegeverklaring, exclusief de bijlagen DigiD en Suwinet opgenomen omdat deze vertrouwelijke detailinformatie bevatten. De verantwoording over DigiD en Suwinet is op hoofdlijnen opgenomen in hoofdstuk 3 van deze jaarrapportage.

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Waterland voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Gemeenten (BIG), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Naast deze verklaring bestaat ENSIA onder meer uit het uitvoeren van de ENSIA-zelfevaluatie, waarmee de genoemde informatiebeveiligingsnormen zijn getoetst onder verantwoordelijkheid van het management.

Reikwijdte en diepgang verklaring

Deze verklaring betreft de onderdelen van de ENSIA-systematiek waarover assurance wordt gevraagd van een onafhankelijke IT-auditor. Het is de verantwoordelijkheid van het college dat het proces voor de totstandkoming van deze collegeverklaring met zorg is uitgevoerd. Dit proces borgt dat de strekking van de collegeverklaring een juiste weergave is van de onderzochte domeinen. Voor gemeente Waterland betreft dit in 2019 DigiD en Suwinet.

De verklaring omvat het op 31 december 2019 voldoen van de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen aan de geselecteerde normen inzake DigiD en Suwinet. De collegeverklaring omvat niet het functioneren (werking) van de maatregelen over 2019.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan de dienstverlener vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD met kenmerk IT20.00659) blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverlener worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverlener worden uitgevoerd, wordt door de dienstverlener verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de normen inzake DigiD af.

Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan GR-BVO Halte Werk (Zelfstandigenloket).

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De verklaring geeft weer in hoeverre de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet. In de bij deze verklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk IT20.00659) en Suwinet (bijlage 2 Suwinet met kenmerk IT20.00660) zijn de eventuele afwijkingen van de normen opgenomen.

De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet worden via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk IT20.00659) en voor Suwinet (bijlage 2 Suwinet met kenmerk IT20.00660) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente Waterland op 31 december 2019 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD.

Het college verklaart dat voor Suwinet niet aan alle geselecteerde normen wordt voldaan. De op de uitzonderingen gerichte beheersmaatregelen zijn in een verbeterplan opgenomen, zijn belegd en worden gemonitord.

Samenvattend beeld

Object	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 999913 Suwinet voor SUWI-taken	Ja Ja	Neen Neen
Suwinet voor niet-SUWI-taken	Neen	Ja

Monnickendam, 7 april 2020

College van burgemeester en wethouders gemeente Waterland