Informatiebeveiliging &Privacy Beleid 2023

Auteur : F. Pijnenborg, CISO
N. Hofstetter, Privacy Officer
Datum : 1 november 2023

Versiebeheer

Versie	Auteur	Beoordelaar	Datum
1.0	F. Pijnenborg, CISO N. Hofstetter, PO	B. Boersma, FG	16/10/2023

Inhoud

1. Inleiding

Onder informatiebeveiliging & Privacy (IB&P)wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening en verwerking van persoonsgegevens aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.
Het IB&P beleid geldt voor alle processen van BghU en borgt daarmee de informatievoorziening en verwerking van persoonsgegevens gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het bestuur, alle medewerkers, burgers, belastingplichtige, gasten, bezoekers en externe relaties.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt IB&P steeds complexer en noodzakelijker. BghU is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft en compliant te zijn aan nationale en Europese wet- en regelgeving op het gebied van IB&P.

Geldigheidsduur
Dit beleid is vastgesteld door het bestuur van BghU, eindverantwoordelijk voor IB&P. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig eerder herzien wanneer er zich wijzigingen met impact voordoen.

2. Visie

De visie van BghU is een goede en betrouwbare dienstverlening met een efficiënt objectenbeheer. Een goed Informatie Security Management Systeem (ISMS) en Privacy Informatie Management Systeem (PIMS) is noodzakelijk voor het goed functioneren van BghU en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor IB&P binnen BghU.

3. Doel van het IB&P beleid

De belastingplichtigen moeten erop kunnen vertrouwen
dat BghU haar informatiebeveiliging en Privacy op orde heeft
voor verwerking van hun persoonsgegevens
en dat wij als BghU relevante wet- en regelgeving naleven.

Met dit IB&P beleid geeft BghU een kader voor het verantwoord omgaan met (persoons)gegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan BghU (persoons)gegevens verwerkt (of laat verwerken). Daarnaast beoogt dit IB&P beleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen voor een effectieve samenwerking om te voldoen aan de AVG.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen BghU, zoals hoofdprocessen en deelprocessen (zie bijlage F).
Iedereen werkzaam binnen BghU is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. BghU verlangt van al haar medewerkers en alle personen die werkzaam zijn voor BghU dat de voorschriften van dit IB&P beleid worden opgevolgd en actief worden uitgedragen.

4. Reikwijdte

De scope van het IB&P omvat alle BghU processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de belastingsamenwerking en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit IB&P beleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en basisregistraties) en DigiD met norm B.01 eisen. Deze worden in aanvullende deelprocessen geformuleerd.

5. De 10 principes voor informatiebeveiliging

Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1. Bestuurders bevorderen een veilige cultuur

Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium. Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als je een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kan de organisatie adequaat reageren op dreigingen en samenhangende risico's.

2. Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement. Iedereen moet betrokken worden bij informatiebeveiliging, in alle lagen van BghU. Maak gebruik van de kennis en verantwoordelijkheid van proceseigenaren en - beheerders. Goed uitgevoerd risicomanagement creëert waarde voor BghU omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3. Informatiebeveiliging is risicomanagement

Informatiebeveiliging wordt bewust toegepast bij alle BghU activiteiten. Informatiebeveiliging werkt alleen als het geïntegreerd is in alle werkprocessen van BghU. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek krijgen in alle bestuurlijke documenten. Proceseigenaren zijn verantwoordelijk voor informatiebeveiliging door afspraken te maken en de nakoming te monitoren. Procesbeheerders zijn verantwoordelijk voor uitvoering van de maatregelen en rapportage over de performance van het proces.

4. Informatiebeveiliging is onderdeel van de besluitvorming

De informatiebeveiliging moet passen bij BghU en de organisatie ondersteunen op beschikbaarheid, integriteit en vertrouwelijkheid conform BghU doelstellingen.
Als bestuur en directeur van BghU geef je de juiste richting wat nodig in relatie tot de activiteiten van de organisatie. Door dreigingen en risico's mee te nemen in de vragen die je stelt aan managers ontstaan er inzichten die meewegen in de besluitvorming van informatiebeveiliging. Zo kun je tijdig bijsturen voordat risico's manifest worden en escalatie voorkomen.

5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

De informatiebeveiliging staat in verhouding tot de externe en interne context van BghU die verband houdt met haar doelstellingen. De keten is zo sterk als de zwakste schakel. BghU dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6. Informatiebeveiliging is een proces

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van BghU verandert. Informatiebeveiliging detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier. Informatiebeveiliging moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen
veranderen, de omgeving verandert en wetgeving verandert. Voor een effectieve informatiebeveiliging houdt BghU rekening met een veranderende omgeving waarmee beheersmaatregelen, op termijn wellicht, doeltreffend en doelmatig.

7. Informatiebeveiliging kost geld

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle maatregelen zijn kosten verbonden. Risico's kan BghU ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve en/of correctieve maatregelen. Voor beheersmaatregelen zal derhalve een kosten-batenanalyse worden gemaakt van de benodigde middelen in capaciteit en geld.

8. Onzekerheid dient te worden ingecalculeerd

De input voor informatiebeveiliging is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden uitgedrukt in een geclassificeerd risico. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden. Met een adequate beschikbaarheid van voldoende informatie kunnen goede risico-inschattingen en besluiten worden genomen met acceptabele rest-risico's voor BghU.

9. Verbetering komt voort uit leren en ervaring

Informatiebeveiliging wordt voortdurend verbeterd door leren en ervaringen. Informatiebeveiliging ontwikkelt zich het beste voor BghU door te leren van ervaringen en op basis hiervan adequaat verbeteringen door te voeren. Hoe goed wij onze informatiehuishouding ook beveiligen, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren werkt BghU doorlopend aan het verhogen en professionaliseren van haar digitale weerbaarheid.

10. Het bestuur controleert en evalueert informatiebeveiliging

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen. Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn binnen BghU. Naast verslagen en managementrapportages zijn incidenten, en hoe zij zijn afgewikkeld, een goede graadmeter om te zien hoe BghU omgaat met informatiebeveiliging. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.

6. Principes Privacy

De AVG is gebaseerd op 6-tal principes voor de verwerking van persoonsgegevens. De organisatie onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

1. Rechtmatige verwerking

Persoonsgegevens worden door de organisatie slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een organisatie voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

2. Doelbinding

De organisatie verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de organisatie alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De organisatie ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.
Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De organisatie voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

3. Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de organisatie bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de organisatie bij voorkeur voor die mogelijkheid.

4. Juistheid

De organisatie zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. De organisatie neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

5. Opslagbeperking

De organisatie stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Organisaties hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

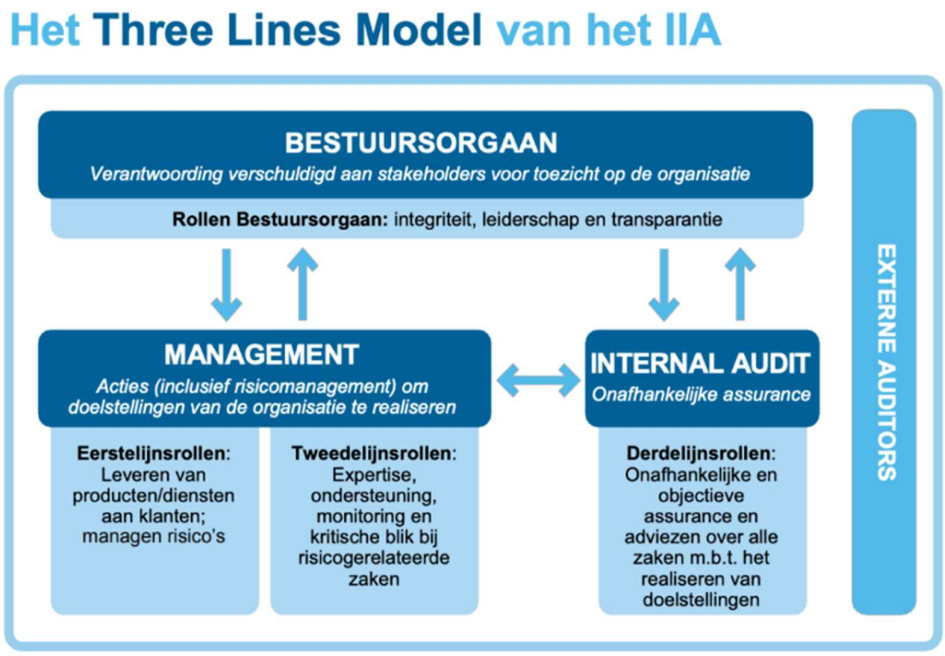
Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de organisatie de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De organisatie bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

6. Integriteit en vertrouwelijkheid

De organisatie neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De organisatie handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de organisatie om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

7 Governance

Het governance model van BghU biedt een overkoepelende visie en strategie hoe de taken en verantwoordelijkheden voor informatiebeveiliging effectief zijn belegd binnen de organisatie. Voor de verdeling van de verantwoordelijkheden van het management en de functies binnen BghU is gekozen om dit in te richten op basis van het "Three Lines Model[1]". Dit model biedt een eenduidige risicotaal en meer transparantie hoe verantwoordelijkheden zijn belegd. Het draagt bij aan versterking aan de accountability voor risicobewustzijn en interne beheersing tussen 1e en 2e lijn.



Organisatie en rollen

Binnen het Three Lines Model zijn de volgende functies en rollen voorzien.

a) Bestuursorgaan: Bestuur
b) Management: Directeur en managementteam
c) 1ste lijn: Managers Dienstverlening, Waardebepaling en Data beheer
    a. Organisatie: Proceseigenaars, Procesbeheerders, Processpecialisten,
d) 2de lijn: Manager Bedrijfsvoering
    a. Organisatie: Privacy Officer & CISO
e) 3de lijn: Interne Controle
    a. Organisatie: FG
    b. Externe auditor (bijv. accountant)

Deze rollen worden hieronder toegelicht.

Bestuursorgaan: Bestuur

Het bestuur is eindverantwoordelijk voor IB&P, het realiseren van opgedragen doelen en het beheersen van risico's.

Het bestuur:

- stelt het IB&P beleid vast;
- bepaalt de risicobereidheid en voert controle uit op het risicomanagement en naleving;
- zorgt voor de benodigde financiële middelen voor de beleidsuitvoering;
- vraagt om transparante verantwoording en aantoonbaar "in control" zijn;

[1] Bron; Institute for Internal Auditors (IIA)

- legt verantwoording af aan externe toezichthouders;
- bevordert een professionele kwaliteit, compliance- en risicocultuur.

Management: directeur en managementteam[2]

1. De ambtelijke organisatie staat onder leiding van de directeur.
2. De directeur heeft de taken en bevoegdheden, genoemd in de artikel 21 en 39 van de regeling en de taken en bevoegdheden die verband houden met de leiding van de ambtelijke organisatie bedoeld in het eerste lid. De directeur heeft in elk geval de volgende taken:
    a. dagelijkse aansturing de ambtelijke organisatie;
    b. zorg dragen voor de inhoudelijke kwaliteit van de taakuitvoering en de dienstverlening;
    c. besluiten over de inzet van en het beheren van middelen;
    d. bijstaan en adviseren van het bestuur, en de voorzitter bij de uitoefening van hun taken, en
    e. bewaken van de eenduidigheid in het functioneren van de Samenwerkingsverband als geheel en het borgen van de verbinding met vertegenwoordigers van de deelnemers.
3. De directeur vormt samen met de managers het managementteam. Het managementteam heeft een periodiek overleg over strategische en tactische onderwerpen.
4. De directeur en het managementteam worden bijgestaan door de eenheid Staf en in het bijzonder de businesscontroller.

1ste lijn: Dienstverlening, Waardebepaling en Data beheer

De 1e lijn is primair verantwoordelijk voor de dienstverlening van de BghU. Daarbij hoort ook het voldoen aan de wet- en regelgeving en volgen van het IB&P beleid.
De verantwoordelijkheden van de 1e lijn zijn:

- Het toepassen en het opvolgen van het IB&P beleid;
- Het toepassen van het processen en deelprocessen IB&P;
- Zorgt dat een hoofdproces geschikt is voor het beoogde doel, voldoet aan wet- en regelgeving en legt hierover verantwoording af;
- stelt de eisen aan continuïteit en betrouwbaarheid voor (delen van) hoofdprocessen vast in relatie tot beschikbaarheid, integriteit en vertrouwelijkheid;
- zorgt dat concrete procesrisico's in beeld zijn en worden beheerst met passende maatregelen;
- laat risico gestuurd interne controles uitvoeren op het hoofd- en deelprocessen;
- zorgt dat capaciteit en middelen beschikbaar komen voor het hoofdproces;
- wijst een procesbeheerder aan om het hoofdproces in te richten en te sturen;
- eindverantwoordelijk voor informatiebeveiliging en privacy binnen het hoofdproces.

De Proceseigenaar (rol) is eindverantwoordelijke voor de volgende taken:

- zorgt dat een hoofdproces geschikt is voor het beoogde doel, voldoet aan wet- en regelgeving en legt hierover verantwoording af;
- stelt de eisen aan continuïteit en betrouwbaarheid voor (delen van) hoofdprocessen vast;
- zorgt dat concrete procesrisico's in beeld zijn en worden beheerst met passende maatregelen;
- laat risico gestuurd interne controles uitvoeren op het hoofdproces;
- zorgt dat financiering beschikbaar komt voor het hoofdproces;
- wijst een procesbeheerder aan om het hoofdproces in te richten en te sturen;
- eindverantwoordelijk voor informatiebeveiliging en privacy binnen het hoofdproces.

De Procesbeheerder (rol) is uitvoerend verantwoordelijk voor de volgende taken:

- Ontwerp, wijzigingsbeheer en continue verbeteren van een hoofdproces en bijbehorende deelprocessen en performance indicatoren;

[2] Artikel 3 Organisatieverordening BghU 2020

- Inrichten van een hoofd- en deelprocessen zodat het voldoet aan de gestelde eisen van de proceseigenaar en van wet- en regelgeving;
- Monitoren en bijsturen op juiste uitvoering van een hoofdproces en deelprocessen;
- Verantwoordelijk voor implementatie en uitvoering van het privacy beleid binnen het eigen hoofdproces;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister;
- Betrekt PO en CISO in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens;
- Voert risicoanalyses uit met hulp van processpecialisten;
- Het vroegtijdig signaleren van bedreigingen waaraan bedrijfsinformatie en persoonsgegevens zijn blootgesteld;
- Het analyseren van beveiligingsincidenten en de consequenties die dit heeft voor beleid en te implementeren bijsturing-/beheersmaatregelen. Deze maatregelen bepalen op basis van incidenten, risicomanagement, het baselinebeveiligingsniveau (BBN) en op basis van de kaders van wet- en regelgeving;
- Het vaststellen getroffen maatregelen aantoonbaar worden nageleefd en rapporteert hierover aan de Proceseigenaar.

De Processpecialist (rol) (optioneel) heeft de volgende taken:
- Heeft diepgaande inhoudelijke kennis over een bepaald aandachtsgebied of onderdeel van het hoofdproces of deelproces;
- Onderhoudt zijn/haar deskundigheid, wet- en regelgeving op het specifiek deelproces;
- De procesbeheerder van een proces proactief informeren over wijzigingen op deelprocessen, wet- en regelgeving en voorstellen doen voor bijsturing of optimalisatie;

De Key-User (rol) heeft de volgende taken:
- Eerste aanspreekpunt voor (nieuwe) gebruikers en overige key-users;
- Heeft frequente interactie met functioneel beheer (wisselwerking);
- Zorgt voor een juiste en tijdige communicatie over ontwikkelingen in het taakgebied naar gebruikers en functioneel beheer;
- Opleider en begeleider van gebruikers in het team of proces;
- Neemt deel aan intern en extern gebruikers-/applicatieoverleg;
- Documenteert en accordeert werkinstructies;
- Heeft actieve rol in inventarisatie en het opstellen van procedureaanpassingen, incidentmeldingen en incidentoplossingen;
- Participeert in implementatie- en migratietrajecten;
- Participeert in het opstellen van wijzigingsverzoeken en in het accepteren van functionele specificaties en het functioneel ontwerp;
- Signaleren, melden en oplossen van datalekken;
- Stelt testplannen op en ondersteunt bij proces overstijgende testplannen, voert Gebruikers Acceptatie Test (GAT) uit en geeft adviezen op basis van testresultaten.

2de lijn: Bedrijfsvoering
De 2e lijn ondersteunt, controleert en adviseert de 1e lijn bij het voldoen aan de wet- en regelgeving en het nemen van passende beveiligingsmaatregelen, zoals:

- Het identificeren van risico's bij het verwerken van persoonsgegevens;
- Het periodiek actualiseren van het IB&P beleid bij de herijking van de vastgestelde risicobereidheid;
- Het doelgericht communiceren over risico's binnen en buiten de reguliere risico overlegstructuur;
- Het proactief aandragen van verbetervoorstellen bij de 1e lijn;
- Een actieve bijdrage leveren aan voorstellen voor de behandeling van risico's en beheermaatregelen die ter goedkeuring worden voorgelegd aan het managementteam;
- Het adviseren en monitoren van verbeteracties (bevindingen o.b.v. beoordeling beheersmaatregelen);
- Het monitoren van de 1e lijn op het naleven van de wet- en regelgeving ter bescherming van persoonsgegevens;
- Het ondersteunen in de opzet en werking, ter bescherming, van persoonsgegevens.

Chief Information Security Officer (CISO)
De CISO definieert het informatiebeveiligingsbeleid en organiseert en stuurt de informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereidheid van de organisatie.

De Privacy Officer (PO)
Het eerste aanspreekpunt voor BghU rondom privacy gerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacy beleid.

3de lijn: Internal Audit
De 3e beheersingslijn wordt gevormd door de onafhankelijke discipline internal audit. De Internal audit helpt BghU haar doelstellingen te realiseren door met een systematische, gedisciplineerde aanpak de effectiviteit van de hoofdprocessen van risicomanagement, beheersing en governance te evalueren en te verbeteren.

Interne Controle
De interne controle regisseert het risico-gebaseerd toezicht op de naleving van wetgeving, intern beleid, maatregelen en procedures zoals dit op de afdelingen uitgevoerd wordt. De interne organisatie van informatiebeveiliging wordt hiervoor onderdeel gemaakt van het Interne Controle-plan. De controle doelstellingen bepaalt de adviseur in overleg met de directie en CISO. Rapporteren over de bevindingen en eventuele benodigde verbeteringen, gaat getrapt via de afdelingsleiding en vervolgens (naar behoefte)aan directie en management.

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG) houdt intern toezicht op het beschermen van persoonsgegevens. De FG onderzoekt en beoordeelt of BghU de AVG naleeft en adviseert (on)gevraagd aan directeur over benodigde verbeteringen.
Externe auditors
Wanneer extra (onafhankelijke) zekerheid gewenst is of geëist wordt door een wet of een toezichthouder, wordt een geaccrediteerd auditor gevraagd om een onderzoek te doen en op basis hiervan een verklaring af te geven.
Hieronder vallen bijvoorbeeld:

a. de accountantscontrole over de jaarrekening;
b. De Digid audit.

8 Control Framework

Voor realisatie van de doelen in dit IB&P Beleid wordt een informatie management systeem ingericht. Dit zijn een managementsystemen gericht op het documenteren, implementeren en evaluatie van maatregelen mbv PDCA-cyclus voor IB&P van BghU.

De opzet van informatie management systeem bestaat uit de volgende elementen;
- Dat informatiebeveiliging wordt opgezet in lijn met de eisen van de BIO;
- Dat overeenkomstig de opzet de verwerkingen en benodigde beheersmaatregelen worden geïmplementeerd;
- Dat technische-, organisatorische- en contractuele maatregelen stelselmatig op hun effectiviteit worden beoordeeld;
- Dat beheersmaatregelen op continue basis worden verbeterd.

De verantwoordelijkheden worden belegd conform de Governance zoals beschreven in hoofdstuk 6 van dit IB&P Beleid.

BghU kan daarmee aantoonbaar voldoen aan de BIO en AVG. Er vinden periodieke rapportages plaats om de opzet, bestaan en werking van het IB&P beleid te monitoren en daarop bij te sturen.

De interne 2e lijn, CISO en PO toetsen elk kwartaal het bestaan en werking van het IB&P beleid. De CISO en PO rapporteren aan de manager Bedrijfsvoering van BghU en zullen op verzoek de rapportage van toelichting voorzien aan verantwoordelijke conform de Governance van dit IB&P Beleid.

De FG rapporteert onafhankelijk elk kwartaal de naleving van de AVG op basis van uitgevoerde audits (opzet, bestaan en werking).

9 Bijlage;

Begrippenlijst

AP: De Autoriteit Persoonsgegevens is de toezichthoudende autoriteit in Nederland op de Algemene Verordening Gegevensbescherming.
Anonimiseren: het verwerken van persoonsgegevens waarbij de bewerking onomkeerbaar is en de persoon niet valt te identificeren. Vanaf dat moment zijn het geen persoonsgegevens meer en is de AVG niet meer van toepassing.
Beperken van de verwerking: het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken;
Beschikbaarheid; beschikbaarheid of continuïteit van (persoons)gegevens en de mate waarin data toegankelijk en bruikbaar is. Nader uitgewerkt of data ook in de toekomst kan worden geleverd, tijdig kan worden geleverd en dat de data bestand tegen verstoringen;
Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;
BIO: De Baseline informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, organisaties, provincies en waterschappen). Had voorheen iedere overheidslaag zijn eigen baseline, nu is er met gezamenlijke inspanning één BIO voor de gehele overheid.
CISO: Chief Information Security Officer verantwoordelijk voor informatiebeveiliging binnen de organisatie.
Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;
DPIA: DPIA staat voor Data Protection Impact Assessment en wordt in Nederland ook wel de gegevensbeschermingseffectbeoordeling genoemd. Is bij het verwerken van persoonsgegevens sprake van hoge risico's, dan is een DPIA volgens de AVG verplicht. Het doel van de DPIA is vooraf aan de verwerking van persoonsgegevens de risico's te inventariseren en daar vooraf beheersmaatregelen voor te treffen.
FG: Functionaris voor Gegevensbescherming. De functie wordt toegelicht in het hoofdstuk Governance en bijlage.
Gegevens over gezondheid: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon.
Governance: het uitvoeren van beleid, controle, macht, regels en principes van de organisatie.
Inbreuk in verband met persoonsgegevens/datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of door de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
Integriteit; Staat voor de betrouwbaarheid voor dat (persoons)gegevens correct en actueel is en dat er geen informatie of data ten onrechte achtergehouden wordt of verdwijnt.
ISMS: ISMS staat voor Information Security Management System en is een managementsysteem voor beheersing van informatiebeveiliging maatregelen. Het ISMS bestaat voor een deel uit IT onderdelen, maar daarnaast komt ook het gedrag van medewerkers, deelprocessen (zie bijlage D) en bedrijfsrichtlijnen aan de orde. Met ISMS wil BghU haar IB verantwoordelijkheden, beheersen en monitoren.
PIMS: PIMS staat voor Privacy Information Management System en is een managementsysteem voor beheersing van privacy maatregelen. Het PIMS bestaat voor een deel uit IT onderdelen, maar daarnaast komt ook het gedrag van medewerkers, standaard procedures (bijv. register van

verwerkingen) en bedrijfsrichtlijnen aan de orde. Met PIMS wil de Organisatie haar privacy verantwoordelijkheden, complementair met informatiebeveiliging, beheersen en monitoren.
Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden gegeven.
Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene");
Profilering: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van de persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met de bedoeling zijn/haar beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;
Pseudonimisering: het verwerken van persoonsgegevens op een zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld. Er worden geen aanvullende gegevens gebruikt, mits deze apart worden bewaard en er technische- en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;
Toestemming van de betrokkene: De burger (betrokkene) heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden;
Vertrouwelijkheid; De mate waarin bevoegdheden en rechten met betrekking tot toevoegen, vernietigen en wijzigen van data op de juiste wijze zijn toegekend, wordt de data voor onbevoegden afgeschermd en worden persoonsgegevens correct verwerkt;
Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke de persoonsgegevens verwerkt;
Verwerking: een bewerking of een geheel van de bewerkingen van de persoonsgegevens, al dan niet geautomatiseerd. Denk hierbij aan het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of het op een andere manier beschikbaar stellen, aligneren of combineren, afschermen, wissen of vernietigen van de gegevens;
Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt.

Relevante wetgeving

Relevante wet- en regelgeving;
- Basisregistraties
- SUWInet
- DigiD
- PUN
- AVG
- Wpg

Standaarden in Informatiebeveiliging
BghU volgt voor het formuleren en realiseren van hun informatiebeveiligingsbeleid de Baseline Informatiebeveiliging Overheid (BIO), afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.
De inhoud en structuur van dit Informatiebeveiligingsbeleid zijn afgestemd op die van de BIO.
Binnen de belastingsamenwerking wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Het beveiligingsbeleid van de belastingsamenwerking is ook voor de bescherming van PA en dit beleid betreft dan ook beleidsafdelingen die zich met PA bezig houden. Voor de bescherming van PA gebruikt de belastingsamenwerking de Cybersecurity Implementatie Richtlijn (CSIR).

IB&P aandachtspunten

Privacy by Default en Privacy by Design
De organisatie houdt bij de ontwikkeling van nieuwe diensten, systemen of hoofdprocessen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt *Privacy by Design* (PbD) genoemd. De organisatie draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de organisatie *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Toegang tot gegevens
Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de organisatie geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De organisatie hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Incidentenmanagement
Informatie uit incidenten, inbreuken op de beveiliging en datalekken
De belastingsamenwerking kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

Inbreuk in verband met persoonsgegevens
Bij toegang tot, verlies of wijziging van persoonsgegevens bij de organisatie, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, binnen 72 uur worden gemeld bij de Autoriteit Persoonsgegevens en bij de getroffen betrokkene. De organisatie registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in het Deelproces Incidentenrespons.

Samenwerking
De organisatie schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de organisatie. De AVG verplicht organisatie tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

Samenwerkingsverbanden
De organisatie werkt samen op diverse gebieden met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkingsverantwoordelijken (gezamenlijk of individueel). De organisatie maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de organisatie.

Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid. In geval er sprake is van doorgifte buiten EER is een Data Transfer Impact Assessment verplicht.

Transparantie
De organisatie informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Voor burgers op de website van de organisatie. Voor medewerkers op het interne Trefpunt. Alleen indien de wet anders bepaalt, wijkt de organisatie van deze informatieplicht af.

Rechten van betrokkenen
Iedereen heeft het recht om te vernemen welke persoonsgegevens de organisatie over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure rechten van betrokkenen.

Geschillenbeslechting
Indien de betrokkene van mening is dat de organisatie niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website van de organisatie. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording
Onder de verantwoordelijkheid van zowel het college van B&W als de organisatieraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de organisatie over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG en WPG intern wordt nageleefd. De organisatie stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

Verwerkingsregister
De organisatie beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt. Hierbij wordt gebruikt gemaakt van het Privacy Information Management Systeem (PIMS)

Data Protection Impact Assessment (DPIA)
Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de organisatie een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De organisatie voert in dat geval een DPIA uit. Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de organisatie voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de organisatie met de AP overleggen, voordat zij met de verwerking start.

Bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn (awareness) in de organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

Privacy Officer (PO)

De Privacy Officer is het eerste aanspreekpunt voor de organisatie rondom privacy gerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacy beleid.

De Privacy Officer heeft de volgende taken en verantwoordelijkheden:

- Adviseert en faciliteert de organisatie ten aanzien van het naleven en de uitvoering van het privacy beleid;
- Beheert het Privacy Informatie Management Systeem (PIMS) inclusief het register van verwerkingen;
- Opstellen privacy beleid en modellen, formats en standaard-overeenkomsten, waaronder bijvoorbeeld de verwerkersovereenkomst voor uitwisseling van persoonsgegevens;
- Monitort, ondersteunt en rapporteert de 1e lijn bij toepassing, opvolging en uitvoering van het privacy beleid;
    - Over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO;
    - In het registreren van verwerkingen in het verwerkingsregister en registreren van relevante wijzigingen;
    - Over de verwerkingsgrondslagen (bijvoorbeeld over toestemming van betrokkene);
    - Het uitvoeren van (pré-)DPIA's en de daaruit voortvloeiende risico's en het nemen van organisatorische- en technische maatregelen;
    - Over de bepalingen in verwerkersovereenkomsten met verwerkers en faciliteert bij het opstellen daarvan;
    - Over mechanismen voor verwerkingen van persoonsgegevens buiten de EU/EER;
    - Over de overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Ontwikkelt de bewustmakingsprogramma's- en privacy trainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Ondersteunt en faciliteert de organisatie bij het beoordelen en afhandelen van datalekken en verzoeken van betrokkene;
- Stelt een werkprogramma privacy jaarplan op voor implementatie en monitoring naleving van de AVG;
- Rapporteert op kwartaalbasis aan de manager Ondersteuning conform Control Framework.

CISO

De Chief Information Security Officer (CISO) definieert het informatiebeveiligingsbeleid en organiseert en stuurt de informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereidheid van de organisatie.

Verantwoordelijkheden;

• Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen
• Het inrichten van de informatiebeveiligingsorganisatie
• Het coördineren en adviseren bij afhandelen van beveiligingsincidenten
• Afstemming van informatiebeveiliging met andere beveiligingsdomeinen
• Het toezien op naleving van de eisen voor informatiebeveiliging
• Het bevorderen van het informatiebeveiligingsbewustzijn over de hele organisatie
• De voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's
• Het adviseren bij en begeleiden van informatierisicoanalyses

• Het uitvoeren van informatiebeveiligingsassessments
Resultaten;

- Projectportfolio voor informatiebeveiliging
- Organisatiebrede informatiebeveiligingsactiviteiten en -projecten
- Monitoring van de relevante risico's voor de organisatie
- Monitoring van compliance met beleid en wet- en regelgeving
- Gecoördineerde reactie op ernstige informatiebeveiligings- of ICT- incidenten
- Organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatie-beveiliging
- Rapporteert op kwartaalbasis aan de manager Bedrijfsvoering conform Control Framework

Functionaris Gegevensbescherming (FG)

Op basis van de AVG en de WPG is het aanstellen van een FG verplicht voor de organisatie.
De FG is verantwoordelijk voor het toezicht op de naleving van de AVG en WPG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie.
De FG heeft de volgende taken en verantwoordelijkheden in de organisatie:

- Interne toezichthouder, 3e lijn, op de naleving van de AVG en WPG ;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en persoonsgegevensbescherming;
- Draagt privacy beleid actief uit binnen de gehele organisatie en bevordert een cultuur van duurzame persoonsgegevensbescherming;
- Adviseert de organisatie bij privacy klachten en verzoeken van betrokkene;
- Adviseert organisatie ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld op uitgevoerde DPIA's en hoog-risico dossiers;
- Adviseert de organisatie bij datalekken;
- Beschikt over controle- en monitoringbevoegdheden;
- Rapporteert op kwartaalbasis aan directeur.

IB proces en deelprocessen[3]

	Deelproces	Subproces
1.	IB Beleid	Goedkeuring Management
		Implementatie
		Communicatie
2.	Organiseren van Informatiebeveiliging	
		Interne organisatie
3.	Veilig personeel	
		Voorafgaand aan het dienstverband
		Tijdens dienstverband
		Wijziging en beëindiging dienstverband
4.	Beheer van Bedrijfsmiddelen	
		Verantwoordelijkheid van bedrijfsmiddelen
		Informatieclassificatie
		Behandelen van Media
5.	Toegangsbeveiliging	
		Bedrijfseisen voor toegangsbeveiliging
		Beheer van toegangsrechten van gebruikers
		Verantwoordelijkheden van gebruikers
		Toegangsbeveiliging van systeem en toepassing
6.	Cryptografie	
		Cryptografische beheersmaatregelen
7.	Fysieke beveiliging en beveiliging van de omgeving	
		Beveiligde gebieden
		Apparatuur
8.	Beveiliging bedrijfsvoering (ISMS)	
		Bedieningsprocedures en verantwoordelijkheden
		Bescherming tegen malware
		Back-Up & Restore
		Verslaglegging en monitoren
		Beheersing van operationele software
		Beheer van technische kwetsbaarheden
		Overwegingen betreffende audits van informatiesystemen
9.	Communicatiebeveiliging	
		Beheer van netwerkbeveiliging
		Informatietransport
10.	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	
		Beveiligingseisen voor informatiesystemen
		Beveiliging in ontwikkelings- en ondersteunende processen
		Testgegevens
11.	Leveranciersrelaties	
		Informatiebeveiliging in leveranciersrelaties
		Beheer van dienstverlening van leveranciers
12.	Beheer van informatiebeveiligingsincidenten	
		Beheer van informatiebeveiligingsincidenten verbeteringen
13.	Informatiebeveiligingsaspecten van bedrijfscontinuïtsbeheer	
		Informatiebeveiligingscontinuïteit
		Redundante componenten
14.	Naleving	
		Naleving van wettelijke en contractuele eisen
		Informatiebeveligingsbeoordelingen

[3] Conform BIO

Privacy Proces en deelprocessen

	Deelprocessen	**Subprocessen**
1.	Privacy by Design	
		Wijzigingsbeheer
		Beoordelen rechtmatigheid
2.	Verwerkingsregister	
		Verwerkers
		Bewaar en vernietiging van persoonsgegevens
3.	DPIA	
		pre-DPIA
		DPIA template
4.	Datalek beheer	
		Melden van een datalek
		Beoordelen datalek
		Melden aan AP
		Melden aan betrokkene
		Registreren datalek
5.	Rechten van betrokkene	
		Verzoek bevestigen
		Verzoek afhandelen
6.	Gegevensverstrekking	
		Aanvraag document gegevens
		Beoordelen aanvraag
		Verstrekking gegevens
		Veilig delen van data