Jaarverslag privacy BSR 2025

Colofon

Titel	:	Jaarverslag privacy BSR 2025
Opdrachtgever	:	Directeur
Auteur	:	Functionaris Gegevensbescherming en Archief (FG)
Versie	:	1.0

Vastgesteld in de vergadering van het dagelijks bestuur BSR 12 maart 2026

W. van Wikselaar
Voorzitter

G.M. Scholtus, MBA
Directeur

Inhoudsopgave

1 Voorwoord

In 2025 heeft de Functionaris Gegevensbescherming (FG) en Archief op interim basis haar werkzaamheden voortgezet. De FG heeft hierbij regelmatig en intensief samengewerkt met de Chief Information Security Officer (CISO) om een samenhangende aanpak van informatiebeveiliging en privacybescherming binnen de organisatie te waarborgen. Deze samenwerking heeft bijgedragen aan een betere afstemming van beleid, controles en risicobeoordelingen op het gebied van informatiebeveiliging en gegevensbescherming.

De werkzaamheden zijn uitgevoerd binnen de PDCA-cyclus van het Information Security Management System (ISMS). Dit managementsysteem biedt structureel inzicht in de status van de verschillende normen van de Baseline Informatiebeveiliging Overheid (BIO). Door deze cyclische aanpak – Plan, Do, Check, Act – wordt continu gewerkt aan het verbeteren van processen, het signaleren van risico's en het implementeren van corrigerende maatregelen. Hierdoor blijft de organisatie voldoen aan de geldende eisen op het gebied van informatiebeveiliging en privacybescherming.

Per 23 september 2025 is de Baseline Informatiebeveiliging Overheid 2 (BIO2) vastgesteld door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). De BIO2 vormt een vernieuwde en uniformere basisnorm voor informatiebeveiliging en biedt een gemeenschappelijk normenkader voor de gehele overheid. De normen zijn afgestemd op actuele risico's, technologische ontwikkelingen en wettelijke vereisten. Sinds de vaststelling van BIO2 zijn wij intern gestart met de implementatie van de BIO2-normen binnen het Information Security Management Systeem (ISMS) en de bijbehorende informatiebeveiligingsdocumenten. Dit traject is zorgvuldig uitgevoerd en naar behoren afgerond. De invoering van BIO2 heeft geleid tot een betere borging van beveiligingsmaatregelen en een uniformere manier van werken binnen de organisatie. Uit de PDCA-cyclus zijn geen nieuwe onvolkomenheden of tekortkomingen naar voren gekomen, wat aangeeft dat de bestaande processen effectief functioneren en voldoen aan de nieuwe normen.

Het bijgevoegde jaarverslag geeft een overzicht van de belangrijkste bevindingen over het afgelopen jaar, waaronder:

- de voortgang in de implementatie van het ISMS en de BIO2-normen;
- de samenwerking tussen FG en CISO bij het beoordelen en mitigeren van informatiebeveiligingsrisico's;
- de naleving van wettelijke verplichtingen op het gebied van privacy en archiefbeheer.

Daarnaast bevat het verslag aanbevelingen voor het komende jaar, gericht op verdere optimalisatie van processen, versterking van de informatiebeveiligingsmaatregelen en continue monitoring van de naleving van BIO2.
Door deze gestructureerde aanpak blijft de organisatie goed voorbereid op toekomstige uitdagingen op het gebied van informatiebeveiliging en gegevensbescherming, terwijl tegelijkertijd de continuïteit van kritieke processen wordt gewaarborgd.

Tiel, 26 februari 2026

Selsela Sultani
Functionaris Gegevensbescherming en Archief

2 Samenvatting

Conform artikel 38 lid 3 van de Algemene verordening gegevensbescherming (AVG) brengt de Functionaris voor gegevensbescherming (FG) rechtstreeks verslag uit aan het hoogst leidinggevende niveau van de verwerkingsverantwoordelijke. Hiermee wordt de onafhankelijke positie van de FG binnen de organisatie gewaarborgd.

De AVG is formeel in werking getreden op 25 mei 2016 en wordt gehandhaafd sinds 25 mei 2018. De tussenliggende periode van twee jaar was bedoeld als implementatietermijn, zodat organisaties voldoende gelegenheid hadden om hun processen, systemen en beleid in overeenstemming te brengen met de nieuwe privacywetgeving en een juiste toepassing van de regelgeving te waarborgen.

Het algemeen bestuur van BSR heeft op 16 mei 2018 het “Centrale Privacybeleid BSR” vastgesteld.
In het vastgestelde beleid wordt uitgegaan van de “Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Per 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) gekomen.
De BIO is het basis-normenkader voor informatiebeveiliging binnen alle overheidslagen (rijk, provincies, gemeenten en waterschappen), waarbij 2019 als overgangsjaar was ingesteld.
Per 23 september 2025 is de Baseline Informatiebeveiliging overheid 2 vastgesteld als opvolger van de BIO. Het is de vernieuwde basisnorm voor informatiebeveiliging binnen de Nederlandse overheid. De BIO2 biedt een uniformere aanpak en een gemeenschappelijke normenkader voor informatiebeveiliging, waarbij risicomanagement centraal staat. Met de komst van BIO2 is de BIO komen te vervallen. Het versterkt de informatiebeveiliging door betere afstemming binnen ketens van overheden en andere partijen.

Met bovengenoemde toelichting heeft er een herziening van het “Centraal Privacybeleid BSR” plaatsgevonden. Hiertoe is het “Privacybeleid BSR 2025 - 2027” opgesteld in afwachting van vaststelling.

In 2025 zijn de werkzaamheden met het ISMS en de controle op alle maatregelen voortgezet. Binnen de PDCA cyclus zijn hierin geen nieuwe onvolkomenheden naar voren gekomen. Om te voldoen aan de normen van de BIO en de BIO2, gebruikt het systeem enkele verplichte activiteiten waarmee op interval basis per norm een controle plaatsvindt. Hiermee wordt aantoonbaar dat BSR als organisatie op de juiste wijze aandacht en opvolging geeft aan de informatiebeveiliging en privacy.

In de voortgang van de ontwikkeling van procesbeschrijvingen via de Landelijke Lokale Belasting Processen (LLBP) zijn flinke stappen gemaakt. De activiteiten van de LLBP zijn nog steeds ondergebracht in de stichting LLBP. Het aantal deelnemers aan de LLBP is gedurende 2025 wederom gegroeid.

In 2025 heeft BSR haar digitale beveiliging verder versterkt door het gebruik van een Virtual Private Network (VPN) en een uitgebreide controle op Multi-factor Authenticatie (MFA). Dankzij het VPN kunnen medewerkers op een veilige en versleutelde manier verbinding maken met de interne systemen, ook wanneer zij buiten het eigen netwerk werken. De uitgebreide MFA-controle voegt hier een extra beveiligingsslaag aan toe, waarbij gebruikers zich via meerdere verificatiestappen moeten identificeren. Door deze maatregelen zijn de systemen van BSR aanzienlijk beter beschermd tegen ongeautoriseerde toegang en cyberdreigingen, met name bij externe toegang tot het netwerk.

In 2025 heeft BSR binnen de organisatie actief aandacht besteed aan het vergroten van de awareness rondom de Algemene Verordening Gegevensbescherming (AVG) en privacy op de werkvloer.
Hiervoor is een informatieve sessie ontwikkeld waarin medewerkers worden geïnformeerd over hun rechten op het gebied van privacy en over hun verantwoordelijkheden bij het zorgvuldig omgaan met persoonsgegevens. Tijdens deze sessie wordt het belang benadrukt van het beschermen van persoonlijke informatie tegen misbruik, diefstal en ongeautoriseerde toegang.
Daarnaast wordt ingegaan op de rol van AI binnen de organisatie en de bijbehorende aandachtspunten op het gebied van informatiebeveiliging. Hierbij wordt onder andere stilgestaan bij risico’s van dataverwerking, verantwoord gebruik van AI-toepassingen en het naleven van geldende wet- en regelgeving.
Met deze sessie versterkt BSR het bewustzijn en de kennis van medewerkers, zodat privacy en informatiebeveiliging structureel onderdeel blijven van het dagelijks handelen binnen de organisatie.

Concluderend kan, terugkijkend op deze verslagperiode, worden gesteld dat er serieuze stappen zijn en worden gezet op het gebied van de BIO2 en aanscherping van de privacy- en informatiebeveiligings-processen en het creëren van awareness omtrent AVG en privacy. Voor 2026 zal de aandacht vooral uitgaan naar nog meer awareness op deze onderdelen.

3 Ontwikkelingen in 2025

3.1 Visie en ethiek

BSR is een vernieuwende en inclusieve organisatie met een heldere visie en een sterke ethische basis. Wij geloven in transparantie, gelijkwaardigheid en maatschappelijke verantwoordelijkheid. In alles wat wij doen staan respect, integriteit en zorgvuldigheid centraal. Deze uitgangspunten bepalen ook onze kijk op privacy. Wij vragen van belastingplichtigen en samenwerkingspartners uitsluitend de informatie die strikt noodzakelijk is om onze werkzaamheden professioneel en zorgvuldig uit te voeren. Daarbij maken wij bewuste en verantwoorde keuzes over welke gegevens wij verzamelen en hoe wij deze gebruiken.

Met de aan ons toevertrouwde informatie gaan wij uiterst zorgvuldig en vertrouwelijk om. Wij beveiligen gegevens adequaat en verwerken deze uitsluitend binnen de geldende wettelijke kaders en met respect voor de persoonlijke levenssfeer. Ook de persoonsgegevens van onze medewerkers behandelen wij met dezelfde zorg, transparantie en integriteit. Privacy is voor ons geen verplichting op papier, maar een wezenlijk onderdeel van onze organisatiecultuur.

3.2 Privacyontwikkelingen van binnenuit

Binnen BSR is in 2025 gewerkt aan het actualiseren van privacybeleid. Een cruciaal aspect hierbij is informatie en de beveiliging hiervan. Wij kunnen als heffende organisatie niet om informatiebeveiliging en informatiesystemen heen, de informatiesystemen vormen immers het zenuwstelsel van onze organisatie en van de (keten)partners waarmee wij zaken doen. De systemen die gebruikt worden kunnen alleen goed functioneren wanneer de beveiliging ervan op orde is. Dat wil zeggen: wanneer wij ervoor zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie gewaarborgd blijft. Het doel hiervan is de informatie te beschermen tegen interne en externe bedreigingen.

In 2025 is binnen BSR ook gewerkt aan het creëren van privacy bewustwording. Ten behoeve hiervan is een sessie ontwikkeld die als doel heeft het vergroten van het bewustzijn van medewerkers over hoe persoonlijke gegevens worden verzameld, gebruikt, opgeslagen en gedeeld. De sessie omvat het informeren van medewerkers over hun rechten met betrekking tot privacy en het belang van het beschermen van persoonlijke informatie tegen misbruik, diefstal en ongeautoriseerde toegang.

3.3 BIO en BIO2

Voor het uitvoeren van informatiebeveiliging maakt BSR gebruik van de BIO2-normen. De BIO2 werkt met een nieuwe structuur volgens NEN-EN-ISO/IEC 27002:2022. De BIO2 geeft meer ruimte om op basis van een verdergaande risicomanagement zelf te bepalen of bepaalde maatregelen nodig zijn om risico's af te dekken. In dat kader is de insteek van risicomanagement dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging en privacy. Daarnaast is de BIO2 in lijn gebracht met de NIS2-richtlijn, specifiek artikel 21 over cyberbeveiligingsmaatregelen.

Met behulp van het ISMS is in 2025 wederom gewerkt met de PDCA. Hierbinnen zijn geen nieuwe onvolkomenheden naar voren gekomen.

3.3 Audit / assessment

Een privacy audit is een systematisch proces waarbij de privacy praktijken – en beleid van BSR worden geëvalueerd om te bepalen in hoeverre ze voldoen aan de wet- en regelgeving, evenals de effectiviteit van de genomen maatregelen ter bescherming van persoonlijke gegevens. Hiermee worden risico's geïdentificeerd, naleving gewaarborgd en verbeterpunten te signaleren. Informatiebeveiliging en privacy maken onderdeel uit van de jaarlijkse te houden audits en assessment zoals:

- Verbijzonderde interne controle (VIC), intern en check door accountant;
- BAG audit, self-assessment in samenwerking met de gemeenten Montfoort en IJsselstein;
- ISO 9001 certificering door Dekra
- ICT-beveiligingsassessment DIGID, Logius; en
- Kantoorautomatisering 27001, certificering door leveranciers van BSR.

Deze verantwoordingen hebben in de loop van 2025 plaatsgevonden.

3.4 Verwerkers en verwerkersovereenkomsten

In 2025 is met diverse bestaande en nieuwe verwerkers een nieuwe dan wel geactualiseerde verwerkersovereenkomst afgesloten. Een actueel overzicht van deze verwerkers en de bijbehorende overeenkomsten is opgenomen in de ISMS-tool. Door de verwerkers zijn in deze periode geen incidenten gemeld.

3.4 Rechten betrokken

Op de website van BSR (www.bsr.nl) is een privacyverklaring opgenomen waarin informatie wordt verstrekt aan betrokkenen over de verwerking van persoonsgegevens.
BSR hecht grote waarde aan de bescherming van de privacy van gebruikers en waarborgt een veilige, zorgvuldige en transparante omgang met persoonsgegevens. In de privacyverklaring wordt onder meer toegelicht:

- welke persoonsgegevens worden verzameld;
- voor welke doeleinden deze gegevens worden gebruikt;
- op basis van welke grondslagen de verwerking plaatsvindt;
- hoe lang gegevens worden bewaard;
- welke rechten betrokkenen hebben (zoals inzage, correctie, verwijdering en bezwaar).

Daarnaast biedt de website duidelijke mogelijkheden voor het indienen van een verzoek of klacht met betrekking tot de verwerking van persoonsgegevens. Ter ondersteuning hiervan zijn formats opgesteld voor:

- een ontvangstbevestiging van een verzoek;
- een afwijzing van een verzoek;
- een toewijzing van een verzoek.

Ook is een stroomschema ontwikkeld waarin is vastgelegd op welke wijze een verzoek zorgvuldig en conform de geldende wet- en regelgeving wordt behandeld.

In 2024 is de privacyverklaring aangevuld met specifieke informatie over het gebruik van cookies op de website. Hierin wordt toegelicht welke cookies worden gebruikt, voor welke doeleinden en hoe bezoekers hun cookievoorkeuren kunnen beheren.

3.5 Beveiligingsincidenten, datalekken en verzoeken AVG

Met onderstaande tabel wordt inzicht gegeven op de inbreuk van ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens. Maar ook de inbreuk van een ongeoorloofde of onopzettelijke wijziging van persoonsgegevens. Daarnaast geeft het inzicht over de rechten van betrokkenen volgens artikel 13 t/m 22 van de AVG welke zijn toegepast in 2025.

Meldplicht datalekken	**Aantal**	**Toelichting**	**Actie**
Datalekken	1	Ambtshalve vermindering naar verkeerd adres	Afgehandeld
Datalek AP	0	Risico is verwaarloosbaar	
Incidenten			
Incidenten			
Toegangsbeveiliging	0	geen meldingen	-
AVG			
Rechtmatigheid	0	privé adres op zakelijke aanslag	-
Inzageverzoek	0	recht van inzage	-

Genoemde beveiligingsincidenten zijn onderzocht, waarbij bepaald is welke inbreuk van toepassing is en of er sprake is van een beveiligingsincident, sprake is van een datalek of dat het een niet geslaagde poging tot inbreuk betreft. Op basis van deze gegevens kan worden gesteld dat er geen ernstige datalek heeft plaatsgevonden. Bij 1 datalek is een correcte ambtshalve vermindering naar het verkeerd adres van

belastingplichtige gestuurd, deze was namelijk verhuisd. Was dus wel bestemd voor de correcte belastingplichtige. Herstelacties waren afdoende en medewerkers zijn hierop gewezen.

3.6 Governance

Er is een duidelijke structuur ten aanzien van de uitvoering van de AVG. Het dagelijks bestuur heeft een Chief Information Security Officer (CISO), een Archivaris, een Privacy Officer (PO) en een Functionaris voor de gegevensbescherming (FG) aangewezen. Deze onderlinge relaties en verantwoordelijkheden blijken uit de vastgestelde beleidsdocumenten voor informatiebeveiliging en privacy. Hiermee wordt voldaan aan artikel 5 lid 2 van de AVG dat bepaalt dat een organisatie dient te kunnen aantonen 'in control' te zijn aangaande de uitvoering van de AVG.

Uitvoering informatiebeveiliging en privacy

- IB-team : bestaande uit CISO (voorzitter), PO, FG en Archivaris;
  (vergaderen 2 maal per maand tenzij er beveiligingsissues zijn)
- Escalatieteam : bestaande uit directeur (voorzitter), FG, CISO, PO en verantwoordelijke manager;
  (vergaderen alleen bij een datalek)
- Privacy team : bestaande uit directeur (voorzitter), managers, FG, CISO en PO.
  (vergaderen 2 maal per jaar bij voorkeur in mei en november)

3.7 Bewustwording

In 2025 is binnen BSR gewerkt aan het vergroten van de privacybewustwording. Ten behoeve hiervan is een sessie ontwikkeld met als doel het bewustzijn van medewerkers te vergroten over de wijze waarop persoonsgegevens worden verzameld, gebruikt, opgeslagen en gedeeld.

Tijdens deze sessie worden medewerkers geïnformeerd over hun rechten op grond van de Algemene verordening gegevensbescherming (AVG) en over het belang van het beschermen van persoonsgegevens tegen misbruik, diefstal en ongeautoriseerde toegang. Daarnaast wordt aandacht besteed aan het belang van veilige online gewoonten, zoals het gebruik van sterke wachtwoorden, het herkennen van phishing- of nep-e-mails en het zorgvuldig omgaan met gegevens die online worden gedeeld. Ook de risico's en kansen van kunstmatige intelligentie (AI) zijn hierin verwerkt. AI biedt ontzettend veel kansen, maar brengt ook specifieke risico's met zich mee op het gebied van informatiebeveiliging en privacy. Zeker binnen een organisatie als BSR, waar gewerkt wordt met persoonsgegevens, is het belangrijk om AI-toepassingen zorgvuldig en verantwoord in te zetten.
De sessie zal in 2026 intern binnen BSR worden verzorgd door de Functionaris Gegevensbescherming (FG).

Daarnaast heeft de FG in 2025 bij het managementteam (MT) aangegeven dat de inzet van een privacy escape room en een e-learningmodule over AVG en privacybewustwording voor alle medewerkers van grote toegevoegde waarde kan zijn. Zowel de interactieve escape room als de digitale leeromgeving dragen bij aan het structureel vergroten van de kennis en bewustheid rondom privacy en gegevensbescherming.
De verwachting is dat deze aanvullende middelen in 2026 aan de medewerkers van BSR zullen worden aangeboden.

Elke nieuwe medewerker doorloopt tijdens de eerste werkweek meerdere modules die aandacht besteden aan onderwerpen zoals informatieveiligheid, integriteit en privacy. Dit vormt een belangrijke basis voor bewustwording op deze thema's. Om deze kennis actief te verankeren en verder te versterken, wordt opvolging gegeven door middel van gerichte awareness-sessies.

3.8 Bewaring en vernietiging versus archiefwet en privacybeleid

De archiefwet en het privacybeleid omvatten de gehele ‘data life cycle’: van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.

In 2025 heeft een nulmeting plaatsgevonden met behulp van de handreiking Kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO). Deze nulmeting is uitgevoerd door het Regionaal Archief Rivierenland (RAR).

Het advies was hierbij om op basis van de resultaten van deze nulmeting een prioritering aan te brengen en de kwaliteitszorg in een jaarcyclus op te nemen. BSR heeft ervoor gekozen de verbeteracties op projectmatige werkwijze aan te pakken. De volgende actiepunten zijn van belang:

- Er zal een kwaliteitssysteem voor informatiebeheer geïmplementeerd worden waarover de archiefinspecteur periodiek geïnformeerd wordt.
- De archiefbescheiden die onder beheer van BSR zijn moeten metagegevens toegekend krijgen.
- Er dient een vervangingsbesluit voor analoge archiefbescheiden genomen te worden.

Opslag en vernietiging van archief vinden tijdig en op wettelijke grondslag plaats. Zo is in 2025 de opdracht gegeven om bepaalde documenten uit het Archief bij BSR volgens de geldende selectielijsten te laten vernietigen. Hetzelfde geldt voor de stukken die in beheer zijn bij het Regionaal Archief Rivierenland.

4 Conclusie en aanbeveling

Het is van groot belang om de bescherming van persoonsgegevens zorgvuldig te borgen. Dit is essentieel, zowel vanuit privacyoverwegingen – om te voldoen aan wettelijke verplichtingen zoals de Algemene verordening gegevensbescherming – als vanuit het perspectief van informatiebeveiliging, om persoonsgegevens te beschermen tegen misbruik, diefstal of ongeautoriseerde toegang.

4.1 Conclusie

Terugkijkend op deze verslagperiode kan worden vastgesteld dat BSR belangrijke stappen heeft gezet op het gebied van informatiebeveiliging en privacy. Met de inrichting van het Information Security Management System (ISMS) kan BSR de richtlijnen van de Baseline Informatiebeveiliging Overheid (BIO) en de BIO2 continu monitoren en naleven, waarmee de organisatie voorloopt op vergelijkbare instellingen.

Daarnaast is er aandacht besteed aan het vergroten van bewustwording bij medewerkers. Nieuwe collega's doorlopen in hun eerste werkweek modules over informatieveiligheid, integriteit en privacy, aangevuld met gerichte awareness-sessies. In 2026 wordt dit verder versterkt door de introductie van een interne privacy-sessie, een e-learningmodule over AVG en privacy, en een interactieve privacy escape room. Hiermee wordt kennis over het veilig omgaan met persoonsgegevens, veilige online gewoonten en de rol van AI binnen informatiebeveiliging actief verankerd binnen de organisatie.
Door deze gecombineerde aanpak borgt BSR niet alleen de bescherming van persoonsgegevens en de naleving van privacywetgeving, maar versterkt de organisatie ook structureel haar informatiebeveiligingspraktijken en de digitale weerbaarheid van medewerkers.

Verder kan worden geconcludeerd dat de essentiële archiefwerkzaamheden binnen BSR gedurende deze verslagperiode conform de geldende wet- en regelgeving zijn uitgevoerd.

Daarnaast hebben zich in 2024 geen noemenswaardige incidenten voorgedaan op het gebied van privacy en informatiebeveiliging, wat aangeeft dat de getroffen maatregelen en bewustwordingsinitiatieven effectief bijdragen aan een veilig en compliant werkklimaat.

4.2 Aanbeveling

Informatiebeveiliging en privacy zijn binnen BSR goed georganiseerd en worden ondersteund door een reeks aantoonbare beheersmaatregelen waarmee de organisatie de naleving van wet- en regelgeving continu kan monitoren en waarborgen. Ook op het gebied van privacy zijn er duidelijke kaders opgesteld, zodat persoonsgegevens veilig worden verwerkt, opgeslagen en gedeeld, in overeenstemming met de Algemene verordening gegevensbescherming (AVG).

Voor 2025 ligt de focus op het verder vergroten van de bewustwording bij medewerkers, zodat informatiebeveiliging en privacy stevig verankerd blijven in het dagelijkse werk. Daarnaast vragen de werkzaamheden die in het verlengde van de Archiefwet worden uitgevoerd de nodige aandacht. Het zorgvuldig beheren, archiveren en raadpleegbaar houden van documenten is essentieel om te voldoen aan wettelijke verplichtingen en om de betrouwbaarheid en traceerbaarheid van informatie te waarborgen.

Terugkijkend op de verslagperiode kan tevens worden vastgesteld dat de essentiële archiefwerkzaamheden conform de geldende wet- en regelgeving zijn uitgevoerd. Bovendien hebben zich in 2025 geen noemenswaardige incidenten voorgedaan op het gebied van privacy en informatiebeveiliging. Dit bevestigt dat de ingezette maatregelen en initiatieven effectief zijn en bijdragen aan een veilige, compliant en bewust werkende organisatie.

Door deze geïntegreerde aanpak borgt BSR niet alleen de bescherming van persoonsgegevens en naleving van relevante wet- en regelgeving, maar versterkt het ook structureel de informatiebeveiligingspraktijken en de digitale weerbaarheid van medewerkers, waardoor de organisatie voorbereid is op toekomstige uitdagingen op het gebied van privacy en cybersecurity.

Bijlage 1

ORGANOGRAM BSR