Privacybeleid Sabewa Zeeland

Geldend van: 13 november 2025 t/m heden

Intitulé

Privacybeleid Sabewa Zeeland

Inhoud

1. Uitgangspunten ... 3
1.1. Voor wie ... 3
1.2. Doel ... 3
1.3. Missie ... 3
2. Reikwijdte ... 4
2.1. Afbakening ... 4
2.2. Uitgangspunten ... 4
2.3. Raakvlakken en overlap met andere beleidsthema's ... 5
2.4. Kapstokregeling ... 5
2.5. Inachtneming bijzondere wettelijke voorschriften ... 5
3. Privacymanagement ... 10
3.1. Taken en verantwoordelijkheden interne organisatie ... 10
3.2. Governance met behulp van three lines of defence Governance model ... 11
4. Transparantie ... 16
4.1. Rechten ... 16
4.2. Vragen ... 16
4.3. Klachten ... 16
5. Privacyvolwassenheid & verplichtingen ... 17
5.1. Gedragsnorm ... 17
5.2. Verwerkingsregister ... 17
5.3. Beheer procesplan ... 17
6. Privacyprogramma ... 22
6.1. Jaarplan privacy ... 22
6.2. Bewustwording en training ... 22
6.3. Pers & communicatie ... 22
6.4. Verdere verwerking, archief en gegevensvernietiging ... 22
6.5. Informatiebeveiliging ... 22
6.6. Regeling inbreuk op de informatiebeveiliging ... 22
6.7. Handhaving ... 22
6.8. Beleidsevaluatie ... 23
7. Auditbeleid ... 24

1. Uitgangspunten

1.1. Voor wie

Het privacybeleid van Sabewa Zeeland (hierna: privacybeleid) stelt de algemene kaders vast waarbinnen de uitvoeringsorganisatie de privacy van personen regelt. Dit beleidsdocument geeft richting en kaders voor nader vast te stellen thematisch beleid en het bevat managementafspraken tussen het bestuur en het managementoverleg. Deze afspraken moeten worden nagekomen in alle gevallen dat persoonsgegevens door Sabewa Zeeland (hierna: Sabewa) worden verwerkt, zoals het gebruik, opslaan of uitwisselen van persoonsgegevens. Daarbij hanteert Sabewa als uitgangspunt en als wettelijke verplichting dat zij behoorlijk en zorgvuldig omgaat met persoonsgegevens in verband met de privacy van betrokkenen. Bescherming van persoonsgegevens is namelijk een grondrecht en daarbij hoort uiteraard een goed stelsel van processen, werkafspraken en overeenkomsten om privacy te waarborgen, maar ook bewustwording, kennisoverdracht en een open en kritische bedrijfscultuur.

Naast het algemene deel bestaat dit beleidsdocument ook uit een nadere uitwerking over de wijze waarop procesplannen voor privacygevoelige werkprocessen tot stand komen en geborgd worden. Hierin geeft de organisatie op uitvoeringsniveau aan hoe zij concreet voorziet in passende organisatorische en technische maatregelen voor de bescherming van persoonsgegevens.

Het privacybeleid is bindend voor iedereen die voor de organisatie werkt of bestuurlijke verantwoordelijkheid draagt.

1.2. Doel

Het doel van het privacybeleid is om te waarborgen dat iedereen binnen de organisatie zorgt voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) en overige geldende wet- en regelgeving.

1.3. Missie

Sabewa waarborgt zorgvuldigheid en veiligheid in het beheer van persoonsgegevens. In een tijd van digitale vooruitgang en globalisering past de organisatie zich aan, met focus op informatiebeveiliging, dataminimalisatie en transparantie. Dit beleid geeft richtlijnen voor het waarborgen, beschermen en handhaven van privacy in de hele organisatie en is in lijn met daarvoor geldende wet- en regelgeving.

2. Reikwijdte

2.1. Afbakening

Het privacybeleid is van toepassing op alle bedrijfsvoeringprocessen, waarbij er gewerkt wordt met persoonsgegevens en de organisatie daar zeggenschap over heeft. De bedrijfsprocessen omvatten ook de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Papieren of digitale informatieverwerking maakt geen verschil. Het beleid is van toepassing op processen die Sabewa uitbesteedt, inkoopt of op een andere manier organiseert en is ook van toepassing op gegevensuitwisseling met zijn deelnemers zoals de gemeenten[1], het waterschap[2] en derden, zoals accountants, notarissen, wettelijke vertegenwoordigers, bewindvoerders of curatoren.

Het privacybeleid omvat 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. Het is van toepassing op de verwerking van gegevens, voor zover personen kunnen worden geïdentificeerd of geprofileerd. Het privacybeleid is ook van toepassing op beveiligingsincidenten waarbij persoonsgegevens zijn gelekt (meldplicht datalekken).

2.2. Uitgangspunten

Sabewa gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. Sabewa houdt zich hierbij aan de volgende uitgangspunten:

- ***Rechtmatigheid, behoorlijkheid, transparantie***. Sabewa verwerkt alleen persoonsgegevens in overeenstemming met de wet en op een behoorlijk en zorgvuldige manier.
- ***Grondslag en doelbinding***. Sabewa zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.
- ***Dataminimalisatie***. Sabewa verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. Sabewa streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
- ***Bewaartermijn***. Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de opgelegde taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.
- ***Integriteit en vertrouwelijkheid***. Sabewa gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt Sabewa voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.
- ***Delen met derden***. In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt Sabewa afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet- en regelgeving. Sabewa controleert de naleving van deze afspraken.

[1] Gemeenten die onderdeel zijn van de gemeenschappelijke regeling: Borssele, Goes, Hulst, Kapelle, Reimerswaal, Sluis, Terneuzen en Tholen.
[2] Het waterschap Scheldestromen.

- ***Subsidiariteit***. Sabewa kiest bij het verwerken van persoonsgegevens altijd voor de meest privacyvriendelijke keuze, waarbij de inbreuk op de persoonlijke levenssfeer van de burger zo klein mogelijk is.
- ***Proportionaliteit***. De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.
- ***Rechten van betrokkenen***. Sabewa honoreert alle rechten van betrokkenen.

2.3. Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid heeft raakvlakken of overlap met andere beleidsstukken. Dit is in ieder geval voor het informatiebeveiligings- en personeelsbeleid.

2.4. Kapstokregeling

Het privacybeleid van Sabewa heeft een algemeen karakter en een raamwerkfunctie (kapstokregeling). Het zoomt niet in op de spelregels die kunnen gelden voor specifieke activiteiten zoals het heffen en innen van de gemeentelijke belastingen en de waterschapsbelasting. Voor zover dit speelt, geven de teammanagers als proceseigenaar, via taakspecifiek beleid en procesplannen nadere invulling aan dit beleidskader.

Het overkoepelend privacybeleid, specifiek beleid, procesplannen en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacybeleid van Sabewa. In geval van tegenstrijdigheid heeft dit overkoepelend privacybeleid van de Sabewa voorrang.

2.5. Inachtneming bijzondere wettelijke voorschriften

Op basis van dit beleid geeft Sabewa uitvoering aan de Algemene Verordening Gegevensbescherming (AVG). Voor zover van toepassing houden proceseigenaren tevens rekening met bijzondere wettelijke voorschriften, met name privacy relevante bepalingen zoals in de Wet basisregistratie personen en de Telecommunicatiewet.

De Algemene Verordening Gegevensbescherming (AVG) is de voornaamste regelgeving waar Sabewa mee te maken heeft in het kader van privacywetgeving. De AVG is rechtstreeks van toepassing in alle lidstaten en heeft rechtstreekse werking. In de Uitvoeringswet op de AVG (UAVG) heeft Nederland haar aanvullende regels op de AVG opgenomen. Tevens gelden nog een aantal andere specifieke regels. Deze worden hieronder besproken. Sabewa voert voor acht Zeeuwse gemeenten en waterschap Scheldestromen wettelijke taken uit. Dit zijn wettelijke taken die voortvloeien uit de Gemeentewet, Waterschapswet en de Wet WOZ. Het gaat hierbij om het heffen en invorderen van gemeentelijke- en waterschapbelastingen en het uitvoeren van de Wet Waardering Onroerende Zaken (Wet WOZ).

Er is een gemeenschappelijke regeling in het leven geroepen waarin Sabewa als zijnde een openbaar lichaam, de uitvoering van deze taken overgedragen heeft gekregen. Sabewa is verplicht haar taken uit te voeren en daarbij persoonsgegevens te verwerken op basis van enkele wetten zoals de Algemene wet inzake rijksbelastingen, Invorderingswet 1990, Gemeentewet, Waterschapswet en de geldende belastingverordeningen van de deelnemende gemeenten en het waterschap. Voor het vaststellen van de WOZ-waarde verwerkt Sabewa persoonsgegevens op basis van de Wet WOZ.

Doordat de bevoegdheden op basis van de bovenvermelde wetten aan Sabewa zijn opgedragen, betekent dit dat zij voor de uitvoering hiervan persoonsgegevens dient te verwerken. Dit ziet op het opleggen van de juiste belastingaanslag, het behandelen van

bezwaar en beroepschriften, het innen en invorderen van de belasting en voor de juiste vaststelling en verstrekking van de waarde van onroerende zaken.

Hiernaast zijn ook nog andere verplichtingen van toepassing. Denk bijvoorbeeld aan de (fiscale)geheimhoudingsplicht uit de Algemene wet inzake Rijksbelastingen en Invorderingswet 1990, maar ook aan de beperkte openbaarmakingsregeling in de Wet WOZ.

Tevens heeft de Sabewa bij de uitoefening van haar taken zich te houden aan:

• De wet Basisregistratie Personen;

• De wet Algemene Bepalingen Burgerservicenummer;

Tenslotte heeft Sabewa zich te houden aan de Baseline Informatiebeveiliging Overheid (BIO2).

3. Visie

Sabewa is een transparante, vooruitstrevende en innovatieve organisatie. Binnen de organisatie wordt veel gewerkt met vertrouwelijke informatie zoals persoonsgegevens van burgers en medewerkers en gevoelige financiële gegevens van burgers en bedrijven. Dat stelt hoge eisen aan medewerkers als het gaat om betrouwbaarheid en integriteit en daarmee dus de zorgvuldige omgang met bedrijfs- en persoonsgegevens. Hiervoor neemt Sabewa conform de AVG passende technische- en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Bescherming van persoonsgegevens en bedrijfsinformatie is essentieel voor de goede dienstverlening.

Op basis van de aard, omvang en risico van verwerking van persoonsgegevens en de ambitie aantoonbaar te voldoen aan de AVG heeft Sabewa haar visie geformuleerd. Zij streeft, binnen het kader van de verwerking van persoonsgegevens, naar een volwassenheidsniveau met de volgende kenmerken:

- De procedures en de processen voor de verwerking van persoonsgegevens worden door middel van interne controles periodiek beoordeeld om na te gaan of deze effectief zijn.
- Het Privacybeleid wordt periodiek (een keer per jaar) herzien om na te gaan of het nog aansluit bij de interne processen binnen Sabewa en de geldende wet- en regelgeving.
- De verschillende beleidsterreinen op het gebied van informatiebeveiliging worden ieder kwartaal gecontroleerd en het informatiebeveiligingsplan wordt minimaal jaarlijks herzien, waarbij wordt gekeken of de genomen maatregelen aan de stand van techniek, de veranderingen in de organisatie, maatschappij en wet- en regelgeving voldoen.
- Het verwerkingsregister wordt minimaal jaarlijks geactualiseerd om een accuraat beeld te geven van te verwerken persoonsgegevens. Verwerkingen die niet meer aan de orde zijn worden uit het register verwijderd en nieuwe verwerkingen worden toegevoegd.
- De wettelijke bewaartermijnen worden toegepast en bewaakt
- Datalekken en (beveiligings)incidenten worden bijgehouden, gerapporteerd en gemonitord.
- Cursussen en trainingen op het gebied van awareness rondom persoonsgegevens voor medewerkers worden minimaal jaarlijks herhaald.

Scope bepalen	Geïntegreerd	Privacy is onderdeel van het verwerken van persoonsgegevens (in ieder relevant proces).
monitoring	Planning en control	PDCA cyclus gestructureerd aanwezig, bijvoorbeeld in jaarplannen
	Directieteam (Strategisch)	Nieuwe ontwikkelingen op het gebied van de privacywet- en regelgeving worden gesignaleerd en verwerkt in de strategische planning van de organisatie

	Management (Tactisch)	Het beleid voor privacy en informatiebeveiliging is geoperationaliseerd naar methodes voor afgewogen keuzes (risico management en kosten/basten voor personen (betrokkenen) en daarna gerealiseerd in maatregelen
	Afdelingen (Operationeel)	Het beleid voor privacy en de classificatie van persoonsgegevens wordt periodiek geëvalueerd op de uitvoering in de praktijk. De gerealiseerde maatregelen worden geëvalueerd en bijgesteld
Aantoonbaarheid	Proceseigenaar is zelf aan zet	Actieve intervisie op best practices, aantoonbare sturing op de AVG, zelf evaluatie, zoekt de FG zelf op voor advies
	FG houdt toezicht op het beleid	Interne en externe audits, DPIA beoordelen, contact met de Autoriteit Persoonsgegevens
	Vastgestelde processen en documentatie	Processen zijn vastgesteld en worden geëvalueerd. Risicoanalyse en regelmatige review. Kwaliteit van resultaten is gedefinieerd (KPI's).
	Kwaliteitsverbetering	Proactieve monitoring op het detecteren van incidenten vindt plaats in het verwerkende proces. Centrale analyse van incidenten en problemen leiden tot verbetering van communicatie.
Mensen	Bewust en aantoonbaar voldoen aan privacy	Leidinggevenden geven voorbeeldgedrag en verbinden consequenties aan ongewenst gedrag. Medewerkers en leiding committeren zich (expliciet) aan het leveren van een bijdrage aan goede informatiebeveiliging en het borgen van privacy.
	Continuïteit in leren	Mensen delen onderling actief kennis, 'best practises' en ervaringen over de omgang met privacy

		en informatiebeveiliging. Meerjarig opleidingsplan.
Inrichting en structuur	AVG beginsel zijn aanwezig (werking)	De AVG beginselen worden altijd gebruikt, administraties zijn inhoudelijk meestal op orde.

4. Privacymanagement

4.1. Taken en verantwoordelijkheden interne organisatie

In dit onderdeel van het privacybeleid wordt de wijze waarop de taken, verantwoordelijkheden en de borging van het beleid binnen Sabewa zijn georganiseerd en belegd uitgewerkt.

Het dagelijks bestuur stelt formeel het privacybeleid vast met inachtneming van de aanbevelingen van de FG, delegeert de uitvoering hiervan aan het managementoverleg en informeert periodiek de raad over de ontwikkelingen van privacy binnen de gemeentelijke organisatie. Het dagelijks bestuur is gezamenlijk verantwoordelijk voor de uitvoering van het privacybeleid en voor controle op naleving van afspraken. Het dagelijks bestuur benoemt een functionaris van de gegevensbescherming (FG) die een toezichthoudende rol vervult op naleving van de privacywetgeving. Een functieprofiel en takenpakket van de FG is vastgesteld.

De directeur geeft sturing aan de uitvoering van het privacybeleid, voorziet in faciliteiten voor bewustwording en training en ziet erop toe dat naleving van dit beleid plaatsvindt. De informatieadviseur is het aanspreekpunt in het managementoverleg als het gaat om de privacybescherming. De juridisch adviseur is namens het managementoverleg belast met coördinerende en faciliterende taken in het kader van de uitvoering van het privacybeleid.

Vanuit een jaarlijks geactualiseerd en vastgesteld jaarplan privacy vindt in afstemming met de juridisch adviseur sturing plaats aan de uitvoering van het privacybeleid en zorgt de functioneel applicatiebeheerder tussentijds voor periodieke voortgangsrapportages en een jaarlijks evaluatierapport (onderdeel van de PDCA-cyclus).

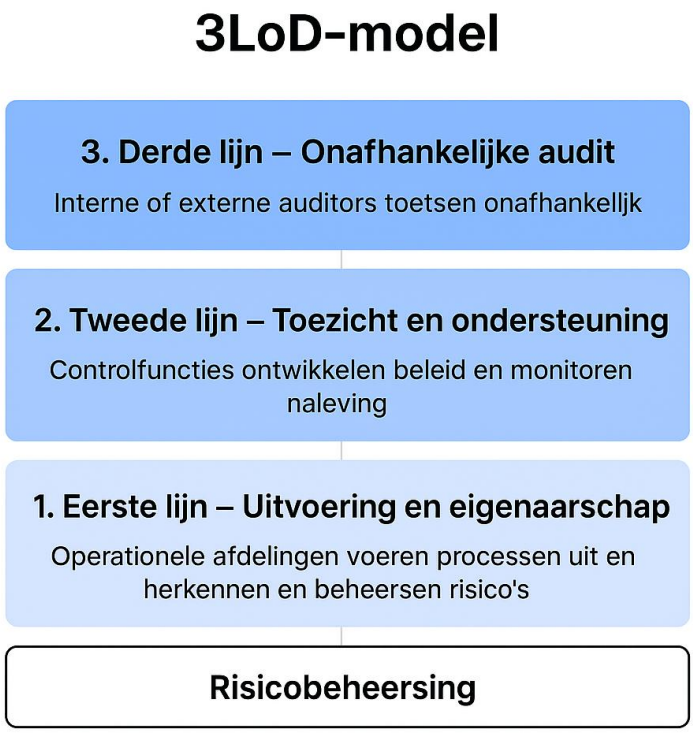
De proceseigenaren zorgen op een aantoonbare wijze dat hun privacygevoelige werkprocessen privacybestendig zijn volgens een daarvoor vastgestelde werkwijze uitmondend in procesplannen. Teammanagers en proceseigenaren maken privacy tot een onderdeel van het werkoverleg. Op deze wijze werkt Sabewa actief aan een open bedrijfscultuur en aan het optimaliseren van kennis en transparante procesuitvoering. Bevindingen of vragen kunnen worden voorgelegd aan de Privacy Officer

De FG heeft een eigen agenda om te toetsen of de aanwezigheid en de werking van het privacybeleid afdoende binnen Sabewa is ingericht. De FG krijgt de nodige ruimte voor de professionele uitvoering van zijn takenpakket, wordt tijdig betrokken bij (wijzigingen in) de verwerking van persoonsgegevens, heeft vrij toegang tot systemen en processen van Sabewa, is adviseur/lid van **het Zeeuws Vlaams FG/PO/CISO overleg** en kan vrij en onafhankelijk rapporteren aan het managementoverleg en het dagelijks bestuur. De zienswijze van de FG is zwaarwegend en geldt als de geëigende wijze voor naleving van privacywetgeving door Sabewa , onverminderd de opvattingen van landelijke toezichthouders.

De wijze van verankering van het privacybeleid binnen Sabewa vormt de basis van de borging van dit belangrijke thema. Op grond van de AVG is het hoogst leidinggevende niveau in de organisatie eindverantwoordelijk voor de rechtmatige en verantwoorde verwerking van persoonsgegevens. Dat is in het geval van Sabewa het Dagelijks Bestuur. Daarnaast draagt elke medewerker in de organisatie, die te maken heeft met verwerkingen van persoonsgegevens, zorg voor de verantwoorde en zorgvuldige omgang met deze gegevens. Ook de proceseigenaren hebben een taak hierin.

4.2. Governance met behulp van three lines of defence Governance model

Voor het bepalen van de taken, verantwoordelijkheden en bevoegdheden met betrekking tot risicomanagement wordt binnen Sabewa het “three lines of defence” model (3LoD model) gevolgd. Dit model beschrijft hoe verantwoordelijkheden voor risicobeheersing belegd worden binnen een organisatie.



Dagelijks bestuur Sabewa

Het dagelijks bestuur draagt de eindverantwoordelijkheid voor informatiebeveiliging en bescherming van persoonsgegevens. Het dagelijks bestuur stelt het Privacybeleid vast en zet hiermee de gekozen richting ter bescherming van persoonsgegevens uit. Het dagelijks bestuur is eindverantwoordelijk voor het toezicht houden en het handhaven van de “three lines of defence”. Het dagelijkse bestuur is eindverantwoordelijk voor naleving van privacywetgeving en:

- Voert proactief het privacybeleid uit op basis van afweging van belangen en risico’s bij de verwerking van persoonsgegevens zodat dit evenwichtig plaatsvindt. Dat wil zeggen, behoorlijk, zorgvuldig en in overeenstemming met de wet;
- Stelt het privacybeleid van de organisatie vast;
- Informeert het algemeen bestuur vanuit de jaarlijkse planning en control cyclus de privacyrisico’s en getroffen beheersmaatregelen binnen de processen waarvoor de organisatie verantwoordelijk is;
- Bevordert dat er voldoende middelen beschikbaar zijn om de bescherming van privacy passend te borgen;
- Benoemt de functionaris voor de gegevensbescherming (FG) zoals bedoeld in artikel 37 AVG zodat onafhankelijk toezicht wordt gehouden op de uitvoering van het privacybeleid;

- Draagt zorg voor een up-to-date beleid en neemt voldoende maatregelen zodat op ieder moment uitleg kan worden gegeven (aantoonbaarheid) over de deugdelijkheid van de aanpak;
- Zorgdragen dat alleen gebruik wordt gemaakt van verwerkers die voldoende garanties kunnen geven voor privacybescherming zoals bedoel in artikel 28 AVG;
- Zorgdragen voor een actueel gegevensverwerkingsregister zoals bedoeld in artikel 30 AVG;
- Zorgt voor het toewijzen van de verantwoordelijkheden ten aanzien van het inrichten, uitvoeren en documenteren van het privacybeleid;
- Stelt de criteria vast voor de aanvaarding van risico's en privacy ambitie niveau;
- Draagt zorg voor het kunnen leveren van bewijs van hun betrokkenheid met betrekking tot het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van beschermen van persoonsgegevens;
- Het dagelijks bestuur wordt over de bescherming van persoonsgegevens periodiek geïnformeerd.

Directeur

De directeur geeft dagelijks leiding aan de organisatie van Sabewa . Hij is ook secretaris van het algemeen bestuur en het dagelijks bestuur.

Afdelingsmanagers/Proceseigenaren rapporteren aan de directeur over hun verantwoordelijkheden in de 1e lijn.

De directeur is ambtelijk verantwoordelijk voor naleving van de privacybescherming en de daarbij behorende algemene sturing en:

- Stuurt de organisatie aan op privacyrisico's;
- Zorgt voor een praktisch uitvoerbare werkwijze voor het periodiek doorlichten van privacygevoelige werkprocessen op privacybestendigheid (tot stand komen en beheren van procesplannen);
- Controleert of de getroffen maatregelen overeenstemmen met de privacyeisen en of deze voldoende bescherming bieden;
- Evalueert periodiek het privacybeleid en stelt waar nodig bij.

Chief Information Security Officer (CISO)

De CISO is gedelegeerd verantwoordelijk namens dagelijks bestuur voor het implementeren van informatiebeveiligingsbeleid én het toezicht daarop. Hij geeft namens het dagelijks bestuur op dagelijkse basis invulling aan de sturende rol door besluitvorming voor te bereiden en toe te zien op de uitvoering. De rol van CISO wordt binnen Sabewa ingehuurd. Binnen de organisatie is er een team belast met de dagelijkste uitvoering van een deel van de taken van de CISO.

Tot de taken van de CISO behoren:

- Het implementeren van het informatiebeveiligingsbeleid én het toezicht daarop. Het opstellen en uitvoeren van een informatiebeveiligingsplan;
- Aandacht besteden binnen de organisatie aan bewustwording met betrekking tot informatiebeveiliging;
- Het borgen van informatiebeveiliging met behulp van het Information Security Management System (ISMS);
- Op verschillende niveaus deelnemen aan overleggen voor signalerend en corrigerend vermogen;
- Periodiek rapporteren aan het dagelijks bestuur en het MT.

Eerste lijn: Teams, teammanagers/proceseigenaren

Uitgangspunt van het 3LoD model is dat de proceseigenaren verantwoordelijk zijn voor hun eigen processen. Om de doelstellingen te realiseren en risico's te minimaliseren zijn beheersmaatregelen opgesteld en vinden allerlei controles plaats. Niet het controleren om het controleren, maar controleren om vast te stellen dat de goede dingen worden gedaan en de doelstellingen niet in gevaar komen. Verantwoordelijkheden van de eerste lijn zijn dan ook:

- Het toepassen en opvolgen van het privacybeleid van Sabewa ;
- Het (mede) onderhouden en opvolgen van het register van verwerkingsactiviteiten;
- Het signaleren en melden van beveiligingsincidenten;
- Het (mede) opstellen en onderhouden van een DPIA en het instellen en monitoren van beheermaatregelen;
- Het controleren en monitoren op de effectiviteit van processen waarbij persoonsgegevens worden verwerkt;
- Bij ontwikkelen van systemen en processen het (mede) toepassen van privacy by design en default;
- Het toepassen van het informatiebeveiligingsbeleid en opvolgen met behulp van technische- en organisatorische maatregelen.

Teammanager/Proceseigenaar

De proceseigenaar is gedelegeerd integraal verantwoordelijk voor processen waar persoonsgegevens worden verwerkt. Inclusief medewerking verlenen aan de daarbij benodigde beheermaatregelen zoals register van verwerkingen, DPIA en verwerkingsovereenkomst met opdrachtgevers en leveranciers.

Teammanagers/proceseigenaren zijn operationeel eindverantwoordelijk voor de uitvoering van de hun toegewezen werkprocessen en:

- zorgen ervoor dat hun privacygevoelige werkprocessen aantoonbaar privacybestendig zijn volgens een daarvoor vastgestelde werkwijze en het bewijs hiervoor hebben vastgelegd in procesplannen;
- documenteren keuzes en oplossingen op een begrijpelijke manier in hun procesplannen;
- onderhouden periodiek hun procesplannen;
- houden regie en toezicht op hun werkprocessen op basis van de specifieke en overkoepelende beleidskaders gericht op privacy;
- handelen vragen of klachten van inwoners of medewerkers binnen 4 weken af conform de klachtenprocedure;
- hanteren de centrale incidentenprocedure bij privacyincidenten;
- zorgen ervoor dat hun privacygevoelige werkprocessen periodiek worden geaudit.

Medewerker van Sabewa

Een eerste lijn/operationeel medewerker draagt bij aan verwerkingen van persoonsgegevens conform AVG. Voor de medewerker van Sabewa schept het privacybeleid zekerheid over de manier waarop hij/zij invulling moet geven aan het privacybelang van de betrokkenen. Hierdoor worden persoonsgegevens één keer goed verwerkt en loopt Sabewa minder risico op reputatieschade.

Tweede lijn: Ondersteuning Controle en Adviseren

Binnen Sabewa is er een team dat de eerste lijn ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt, dit is voor wat betreft de Privacy team Functioneel Applicatiebeheer en de juridisch adviseur. Ook het verzorgen van integrale managementinformatie omtrent risico's en daarover rapporteren is een taak van de tweede lijn.

De tweede lijn omvat de volgende activiteiten;

- Identificeren van risico's bij het verwerken van persoonsgegevens;
- Periodiek het privacybeleid actualiseren op basis van de herijking van de vastgestelde risicobereidheid;
- Het faciliteren van het proces van risicomanagement in de vorm van sessies, formats, tooling;
- Doelgerichte communicatie over risico's organiseren/faciliteren, zowel binnen als buiten de reguliere risico overlegstructuur;
- Het proactief verbetervoorstellen aandragen bij de eerste lijn;
- Een actieve bijdrage leveren aan het formuleren van voorstellen voor behandeling van risico's en het formuleren van beheermaatregelen welke ter goedkeuring worden voorgelegd aan het managementteam;
- Advisering en monitoring van verbeteracties (bevindingen o.b.v. beoordeling beheersmaatregelen);
- Monitoring van de eerste lijn op naleving van wet- en regelgeving ter bescherming van persoonsgegevens;
- Ondersteuning in de opzet en werking ter bescherming van persoonsgegevens.

Ondersteuning eerste lijn op privacy

Team Functioneel Applicatiebeheer ondersteunt, controleert en adviseert de eerste lijn. De taken die hierbij behoren zijn:

- Beheren register van verwerkingsactiviteiten;
- (mede) Opstellen van model verwerkingsovereenkomst/-afspraken;
- Coachen op toepassen en sluiten van verwerkersovereenkomsten/afspraken met derde partijen wanneer deze in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken;
- Opstellen en onderhouden van het privacybeleid en voorleggen ter vaststelling;
- Opstellen privacyverklaring voor betrokkenen;
- Het analyseren van (potentiële) datelekken en zo nodig melden bij Autoriteit Persoonsgegevens en betrokkene(n);
- Coachen op werkinstructies conform aanverwante wet- en regelgeving en beleid van Sabewa ;
- Sturen op integreren privacy in de werkprocessen en de procesbeschrijvingen;
- Opstellen procedures uitoefening rechten van de betrokkenen;
- Ondersteuning eerste lijn bij procesinrichting en werkinstructies;
- Contactpunt binnen de organisatie voor privacyvraagstukken;
- Behandelen verzoeken van betrokkenen ten aanzien van de uitoefening van hun rechten;
- Uitvoeren of sturen op de uitvoering van de DPIA's;
- Periodiek overleg met de FG en de CISO.

Ondersteuning eerste lijn op informatiebeveiliging

- Het onderhouden van de beleids- en kaderdocumenten op het gebied informatiebeveiliging van Sabewa ;
- Het uitvoeren van de informatiebeveiligingsafspraken van de CISO;
- Het maken van risico-analyses op het gebied van informatiebeveiliging;
- Het opstellen van security-ontdekkende systemen;
- Het opstellen van minimum veiligheidseisen en het digitaal rechercheren.

Derde lijn: Toezicht

De derde lijn betreft de toezichthoudende rol. Sabewa heeft een externe Functionaris Gegevensbescherming aangesteld.

Functionaris voor Gegevensbescherming (FG)

De FG is verantwoordelijk voor onafhankelijk toezicht op naleving van relevante wet- en regelgeving, waaronder de AVG, inzake de bescherming van persoonsgegevens en informatiebeveiliging.

1. De taken van de Functionaris voor Gegevensbescherming.
    a. De verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van de AVG en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen.
    b. Toezien op naleving van de AVG en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits.
    c. Desgevraagd advies verstrekken met betrekking tot DPIA's en toezien op de uitvoering daarvan in overeenstemming met artikel 35 AVG.
    d. Met de toezichthoudende Autoriteit Persoonsgegevens samenwerken.
    e. Optreden als contactpunt voor de toezichthoudende autoriteit inzake aangelegenheden die verband houden met verwerking , met inbegrip van in artikel 36 AVG bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.

2. De Functionaris voor Gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

5. Transparantie

5.1. Rechten

Personen hebben er recht op:
- dat Sabewa handelt volgens het onderhavige privacybeleid;
- dat Sabewa informatie verschaft over doelen van informatieverwerking;
- dat zij middels DigiD via de website van Sabewa inzage in hun eigen gegevens hebben;
- dat zij – in geval van fouten – hun gegevens kunnen (laten) verbeteren of verwijderen;
- om tegen het gebruik van hun gegevens verzet aan te tekenen, wat de organisatie verplicht tot het maken van een afweging;
- dat zij de organisatie bij niet-naleving van het privacybeleid (of de wet) hierop mogen aanspreken.

Sabewa respecteert uiteraard ook overige bij wet toegekende privacyrechten.

5.2. Vragen

Bij vragen over privacy:

- hebben personen het recht om zich te wenden tot de klachtencoördinator ;
- richt Sabewa zich op een zo snel mogelijke afhandeling;
- kan de klachtencoördinator de juridisch adviseur belast met privacyvraagstukken of de FG om advies vragen over de beantwoording.

5.3. Klachten

Een niet tot tevredenheid afgehandelde vraag of een directe klacht geeft personen het recht om zich te wenden tot de klachtencoördinator van Sabewa. Voor verdere informatie hierover kunt u de klachtenregeling belastingsamenwerking Sabewa Zeeland raadplegen. Bij een klacht over de verwerking van persoonsgegevens is de klachtencoördinator van Sabewa verplicht om de FG om advies te vragen.

6. Privacyvolwassenheid & verplichtingen

Overeenkomstig de AVG zal de verwerking van persoonsgegevens verantwoord moeten geschieden. Sabewa moet aantoonbaar verantwoord met persoonsgegevens omgaan. Dit wordt ook wel de verantwoordingsplicht genoemd. Hieronder wordt dit toegelicht.

6.1. Gedragsnorm

Het Dagelijks Bestuur verwacht van proceseigenaren rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support van de juridisch adviseur en de FG. Het Dagelijks Bestuur voert ook op andere manieren voorwaardenscheppend beleid teneinde binnen de organisatie een privacybestendige cultuur te realiseren.

Proceseigenaren voorzien in passende organisatorische en technische oplossingen om de rechtmatigheid, proportionaliteit, juistheid en veiligheid van persoonsgegevens te waarborgen (privacywaarborgen) en documenteren die maatregelen in procesplannen.

Het Dagelijks Bestuur en de directeur zijn transparant over de verwerking van persoonsgegevens binnen onder andere de bedrijfsvoering processen, de uitvoering van dit privacybeleid en faciliteren de uitoefening van rechten zoals is besproken in hoofdstuk 4. Proceseigenaren verlenen hieraan hun medewerking.

Het Dagelijks Bestuur, directeur en proceseigenaren dragen het belang uit van privacy en de AVG en geven zelf het goede voorbeeld. Zij maken privacy bespreekbaar. Bij dilemma's gaat Sabewa de dialoog aan met doelgroepen over wie informatie wordt verwerkt.

6.2. Verwerkingsregister

Sabewa treedt op als verwerkingsverantwoordelijke bij hun wettelijke taken. Ook is Sabewa verwerkingsverantwoordelijke als werkgever. Voor deze verwerkingen van persoonsgegevens binnen de organisatie wordt een register van verwerkingsactiviteiten onderhouden. Per team is de proceseigenaar rolverantwoordelijk, gegevensbeheerder, om het register actueel te houden en minimaal eenmaal per jaar te reviewen. Voor begeleiding in deze taak kan de rolverantwoordelijke (proceseigenaar of gegevensbeheerder) een beroep doen op de FG.

De functioneel applicatiebeheerder in samenwerking met de juridisch adviseur zijn belast met het beheer van het verwerkingsregister conform artikel 30 AVG. Proceseigenaren zijn verantwoordelijk voor het jaarlijks actualiseren van de 'eigen' processen. Proceseigenaren melden veranderingen voor het verwerkingsregister onmiddellijk.

6.3. DPIA

In geval van verwerking van persoonsgegevens waarbij sprake is van hoge risico's is een DPIA volgens de AVG verplicht. Het doel van de DPIA is om vooraf de risico's te inventariseren voor de persoonsgegevensverwerking en daar vooraf beheermaatregelen voor te treffen. De proceseigenaar is verantwoordelijk voor het opstellen van een DPIA op een proces.

Voor de uitvoering van een DPIA heeft Sabewa een vast format en een beslisboom DPIA om te bepalen of een DPIA noodzakelijk is.

Advies FG

Als de DPIA is uitgevoerd wint de eigenaar van de DPIA een advies in van de FG. De FG zal de aanwezigheid van hoog risico verwerkingen en bijbehorende beheermaatregelen beoordelen ter bescherming van de rechten en vrijheden van betrokkene.

Monitoring van de beheermaatregelen

De proceseigenaar is verantwoordelijke voor de DPIA en monitort minimaal per jaar de opvolging en effectiviteit van de genomen beheermaatregelen in de DPIA.

Periodieke review DPIA

Als een DPIA is opgesteld, vindt er minimaal binnen 3 jaar vanaf datum vaststelling een review plaats. Doel is vast te stellen of er wijzigingen hebben plaatsgevonden in de verwerking van persoonsgegevens en de genomen beheermaatregelen effectief zijn.

6.4. Bewaartermijnen en -beleid

De AVG schrijft voor dat persoonsgegevens niet langer worden bewaard dan noodzakelijk. Elke gekozen bewaartermijn is mogelijk mits de termijn van noodzakelijkheid voldoende wordt gemotiveerd.

De Archiefwet en de daar mee in verband staande wet- en regelgeving geldt als normenkader voor de door Minister van Onderwijs, Cultuur en Wetenschap goedgekeurde selectielijst met de daar in beschreven bewaartermijnen. De bewaartermijn wordt vastgelegd in het verwerkingsregister. Vervolgens zal de (proces)eigenaar verantwoordelijkheid nemen dat na afloop van de bewaartermijn persoonsgegevens worden verwijderd.

Sabewa streeft er naar dat bewaartermijnen automatisch worden gemonitord. Doch in veel gevallen zal dat niet altijd mogelijk zijn en dient de (proces)eigenaar over het beheer van persoonsgegevens beheermaatregelen in te stellen zodat periodiek de overschrijding van bewaardata wordt gecheckt en persoonsgegevens handmatig worden verwijderd door een verantwoordelijk medewerker. De (proces)eigenaar van persoonsgegevens geeft indien van toepassing autorisatie voor het verwijderen van (persoons)gegevens in het archief.

Geautomatiseerd bijhouden van bewaartermijnen

In de software van applicaties is ingebouwd dat bewaartermijnen automatisch bijgehouden worden. De software biedt de mogelijkheid een vernietigingslijst aan te maken en informatie te vernietigen wanneer de termijn verstreken is.

Handmatige verwijdering

Elke medewerker is verantwoordelijk om periodiek conform afgesproken bewaartermijnen persoonsgegevens handmatig te verwijderen. Er dient dan gecontroleerd te worden of in de digitale afvalbak of verwijderde items (Outlook) de persoonsgegevens ook zijn verwijderd. De proceseigenaren zijn eindverantwoordelijk en zien er op toe dat persoonsgegevens daadwerkelijk worden verwijderd. Hierbij dient ook rekening te worden gehouden met logging en back-ups. De ICT dienstverlener neemt de verantwoordelijkheid persoonsgegevens met betrekking tot logging en back-ups periodiek conform afgesproken termijn te verwijderen. Nadat persoonsgegevens op de bron locatie zijn verwijderd, zullen

de persoonsgegevens nog tijdelijk op back-up media blijven bestaan conform de afgesproken bewaartermijnen. Daarna worden ook de persoonsgegevens op back-up media ook vernietigd.

Monitoring

Periodiek worden bewaartermijnen en beleid gemonitord om met behulp van een analyse te onderzoeken of er andere oorzaken ten grondslag liggen aan het niet opvolgen van vastgelegde bewaartermijnen. Met behulp van deze analyse vindt er dan bijsturing plaats op de gevonden oorzaken om toekomstige overschrijdingen van bewaartermijnen of verstoringen in processen te voorkomen. Voor de exacte bewaartermijnen van persoonsgegevens: raadpleeg het register van verwerkingsactiviteiten.

6.5. Datalekken

Er is een interne procedure ingericht voor het melden van datalekken en beveiligingsincidenten. Een ieder die werkzaam is bij Sabewa kan via deze procedure op een laagdrempelige manier elk (vermoeden van een) datalek of beveiligingsincident melden. De beoordeling of er daadwerkelijk sprake is van een datalek of beveiligingsincident ligt bij de teammanagers en de FG. Er wordt een register van datalekken en van beveiligingsincidenten bijgehouden.De proceseigenaar is verantwoordelijk voor het herstellen van de gevolgen van een datalek of beveiligingsincident en het beoordelen of er maatregelen noodzakelijk zijn om toekomstige datalekken te voorkomen. De proceseigenaar legt dit vast in het register van datalekken. Ieder kwartaal wordt er aan het management gerapporteerd over datalekken en beveiligingsincidenten bij de controle op het incidentmanagement.

6.6. Rechten van betrokkenen

Om een rechtmatige verwerking van persoonsgegevens te waarborgen geeft de AVG diverse rechten aan de betrokkene. De betrokkene kan deze rechten uitoefenen tegen de organisatie als deze optreedt als verwerkingsverantwoordelijke.

In de privacyverklaring op de website van de Sabewa is opgenomen hoe betrokkene beroep kan doen op zijn of haar rechten. Indien Sabewa de verantwoordelijke is voor de verwerking van de persoonsgegevens, kan betrokkene een e-mail sturen naar de organisatie. Vervolgens zal Sabewa de betrokkene binnen 30 dagen informeren over de uitvoering van het verzoek. Ook wanneer er geen gehoor wordt gegeven aan het verzoek van de betrokkene moet dit binnen 30 dagen kenbaar gemaakt worden. Een weigering moet worden gemotiveerd. Tenslotte moet de betrokkene informatie krijgen over het klachtrecht bij de toezichthouder.

Privacy klachten

Elke uiting van onvrede betreffende de verwerking van persoonsgegevens is een klacht. Een klacht kan door een betrokkende of een derde worden geuit, in het geval een derde de klacht indient is het relevant te controleren of deze derde gemachtigd is op te treden namens de betrokkene. De privacyklacht wordt geregistreerd conform de klachtenregeling belastingsamenwerking Sabewa. De afhandeling van een privacyklacht geschiedt altijd in overleg met de FG.

6.7. Beveiligingsmaatregelen

De AVG schrijft voor om rekening houdend met de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context en het doel van de verwerking beveiligingsmaatregelen te treffen. De verwerkingsverantwoordelijke treft technische en

organisatorische maatregelen die passen bij de kans en ernst van uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen die aan de verwerking zijn verbonden. In geval men optreedt als verwerker treft men gelijke beveiligingsmaatregelen als verwerkingsverantwoordelijke. Sabewa heeft de onderstaande technische en organisatorische maatregelen getroffen op basis van de Baseline Informatiebeveiliging Overheid (BIO2). Dit betreft het normenkader voor overheidsorganisaties op het gebied van informatiebeveiliging.

• *Technische maatregelen*

Een procedure op basis van (PDCA) Plan, Do, Check, Act voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

• *Organisatorische maatregelen*

- Informatiebeveiligingsbeleid Sabewa (strategisch en tactisch).
- Beschikbaarheid, Integriteit, Vertrouwelijkheid risicoanalyse op systemen, processen en diensten.

  Het vermogen om op permanente basis de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkingssystemen en diensten te garanderen.
- Business continuïteit management (BCM).

  Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
- Geheimhoudingsverklaring

  Als er sprake is van een externe medewerkers tekent hij/zij voor indiensttreding of het aangaan van de werkrelatie met Sabewa een geheimhoudingsverklaring.

Autorisatie van medewerkers

In het kader van bescherming van persoonsgegevens hebben medewerkers autorisaties om persoonsgegevens te raadplegen en/of te muteren. Vanuit een rollenmatrix worden autorisaties toegekend in processen voor de raadpleeg- en/of mutatiefunctie. Hierbij wordt vooraf beoordeeld of een functie beschikt over de juiste rollen en niet meer persoonsgegevens kan verwerken dan noodzakelijk. Er kan sprake zijn van een inbreuk/datalek als een medewerker ongeoorloofd persoonsgegevens kan raadplegen. De proceseigenaar is eindverantwoordelijk om de rollen toe te kennen in processen en de noodzakelijkheid vooraf te beoordelen. De leidinggevende van een medewerker is verantwoordelijk om de medewerker bij indiensttreding op basis van zijn functie en taken de beschikking te geven over de juiste rollen.

6.8. Awareness

Voor een effectieve werking van het privacybeleid is voldoende awareness van management en medewerkers van belang bij het verwerken en beschermen van persoonsgegevens. Dit is bepalend in de effectieve werking van technische- en organisatorische maatregelen. De effectiviteit van awareness wordt bepaald door de kennis van medewerkers op het gebied van beschermen van persoonsgegevens en hun handelen bij verwerkingen van persoonsgegevens. Tijdens het arbeidsvoorwaardengesprek wordt het belang van integriteit en geheimhouding benadrukt en wordt aan medewerker gemeld dat

hij/zij de eed/gelofte moet afleggen. De eed/gelofte wordt na indiensttreding afgelegd, waarbij de gedragscode wordt uitgereikt en besproken.

7. Privacyprogramma

7.1. Jaarplan privacy

De directeur stelt jaarlijks een jaarplan privacy vast, mede op basis van de jaarrapportage van de FG en de aanbevelingen die de FG hierin doet. Het jaarplan privacy is vooral gericht op het realiseren en in stand houden van een privacyvolwassen bedrijfscultuur binnen Sabewa , met gebruikmaking van overige instrumenten die in deze paragraaf worden beschreven.

7.2. Bewustwording en training

De directeur bevordert samen met proceseigenaren een privacy bewuste organisatiecultuur via voorbeeldgedrag en door te voorzien in de middelen voor bewustwording en, zo nodig, training van medewerkers en leidinggevenden. Hiervoor zal maakt Sabewa gebruik maken van een nog op te stellen onderwijs- en communicatieplan.

7.3. Pers & communicatie

De directeur is transparant over de uitvoering van het privacybeleid en voert op dit thema evenwichtig communicatiebeleid waarbij de teammanagers zo nodig voorzien in bijzondere voorlichting aan specifieke doelgroepen.

7.4. Verdere verwerking, archief en gegevensvernietiging

De directeur voorziet samen met proceseigenaren in met passende waarborgen omklede verdere verwerking van gegevens voor verenigbare doelen zoals het genereren van managementinformatie. Ook wordt voorzien in met passende waarborgen omklede oplossingen voor archivering en adequate oplossingen voor gegevensvernietiging.

7.5. Informatiebeveiliging

Het Dagelijks Bestuur ziet erop toe dat het informatiebeveiligingsbeleid van Sabewa in lijn met de geldende norm wordt georganiseerd. Sabewa beschikt over een gekwalificeerde coördinerende informatiebeveiliger (CISO) die samenwerkt met de directeur en de FG. Geheimhoudingsverklaringen zijn instrumenten binnen de gemeentelijke aanpak voor privacybescherming en informatieveiligheid. Bij processen in de klassen C2-3, B2-3, A2-3 (zie bijlage 1) worden aanvullende geheimhoudingsafspraken gehanteerd voor zover uit de DPIA’s blijkt dat extra waarborgen op het gebied van vertrouwelijkheid/geheimhouding functioneel zijn.

7.6. Regeling inbreuk op de informatiebeveiliging

De directeur voorziet in een procedure voor incidenten met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid zoals opgenomen in het informatiebeveiligingsbeleid. Ook wordt er voorzien in een aparte procedure voor datalekken. Sabewa maakt hiervoor gebruik van het beleid datalekken als onderdeel van het indicentmanagementbeleid.

7.7. Handhaving

De FG is als onafhankelijk toezichthouder degene die zorgdraagt voor de controle op de naleving van de AVG en aanverwante privacyregelgeving door Sabewa . Indien de FG hiaten of onrechtmatigheden constateert, rapporteert de FG dit aan de proceseigenaar en

informeert de directeur. Indien de proceseigenaar het advies van de FG niet opvolgt, rapporteert de FG dit aan de directeur en indien vereist aan het Dagelijks Bestuur.

7.8. Beleidsevaluatie

Proceseigenaren doen binnen de pdca-cyclus verslag aan het bestuur over de naleving van het privacybeleid, oplossingen en incidenten die onder hun verantwoordelijkheid hebben voorgedaan met afschrift aan de FG. De FG verzorgt periodiek het verslag aan het bestuur en geeft aanbevelingen die strekken tot verdere optimalisering van het privacybeleid. Het bestuur besluit over bijsturing van het privacybeleid met inachtneming van de aanbevelingen van de FG.

8. Auditbeleid

Klachten en privacy/beveiligingsincidenten zijn in feite een graadmeter als het gaat om de kwaliteit van de naleving van de privacywetgeving. Uiteraard is het van belang om klachten en incidenten zoveel mogelijk te voorkomen en om niet voor onaangename verrassingen te worden geplaatst. Daarom is periodieke toetsing van de beleidsvoering in relatie tot de feitelijke situatie als onderdeel van de PDCA-cyclus van groot belang en zeker voor die onderdelen waarbij het privacyrisico hoog is. Bij elk procesplan zijn dan ook ijkpunten in de vorm van keycontrols gedefinieerd die periodiek getoetst (privacyaudits) behoren te worden. De verantwoordelijkheid hiervoor ligt bij de proceseigenaren.

Voor privacyaudits onderkennen we 3 typen te weten een:

- quick scan ofwel een beknopte toets onder de verantwoordelijkheid van de proceseigenaar;
- zelfevaluatie ofwel een uitgebreidere toets onder de verantwoordelijkheid van de proceseigenaar;
- audit waarbij sprake is van een onafhankelijke beoordeling die de proceseigenaar organiseert in samenwerking met de FG en waarbij eventueel een professionele externe auditor wordt betrokken.

Voor werkprocessen (zie bijlage 1) die onder C3 vallen geldt een audit met een frequentie van om de 2 jaar. Voor werkprocessen die onder A3, B3, C1 en C2 geldt eveneens een audit maar met een frequentie van om de 3 jaar. Voor werkprocessen onder A2, B1 en B2 geldt een zelfevaluatie om de 5 jaar en voor A1 een quick scan om de 5 jaar.
De FG is bij alle audits betrokken en bij audits is hij mede-ontvanger van het auditrapport.

Besluit

Aldus vastgesteld in de vergadering van het Dagelijks Bestuur van Sabewa op 13 november 2025.

mr. drs. A.J.G. Poppelaars,	dhr. E.H.J. van den Dobbelsteen MSc,
Voorzitter	Directeur

9. Bijlage 1

Behorend bij de hoofdstukken 7.5 en 8 Overzicht FG-controleaudit – Toetsingsonderwerpen

Code	Hoofdonderwerp	Controlepunt / Wat wordt beoordeeld	Toelichting voor de FG-audit
A1	**Beleid voor gegevensbescherming**	Is er een formeel vastgesteld privacybeleid binnen de organisatie?	Het beleid moet actueel, goedgekeurd door bestuur/college en afgestemd zijn op AVG en BIO.
A2	**Organisatie en verantwoordelijkheden**	Zijn taken, bevoegdheden en verantwoordelijkheden rond privacy duidelijk belegd?	Denk aan rollen van FG, CISO, verwerkingsverantwoordelijke, proceseigenaren.
A3	**Toepassing wet- en regelgeving (AVG, UAVG, sectorwetgeving)**	Wordt voldaan aan relevante wet- en regelgeving?	Controle op naleving van de AVG, bewaartermijnen, rechten van betrokkenen, DPIA's, verwerkersovereenkomsten, etc.
B1	**Risicoanalyse en DPIA**	Worden privacyrisico's periodiek geïnventariseerd en beoordeeld?	Bijvoorbeeld via Data Protection Impact Assessments (DPIA's) en risicoregisters.
B2	**Behandeling van risico's**	Worden maatregelen getroffen op basis van de uitkomsten van risicoanalyses?	Gaat om aantoonbare opvolging van risico's (mitigerende maatregelen, verantwoordingsplicht).
C1	**Beveiligingsmaatregelen (technisch & organisatorisch)**	Zijn adequate beveiligingsmaatregelen getroffen en onderhouden?	Denk aan encryptie, logging, patchmanagement, fysieke beveiliging, toegangsbeheer.
C2	**Toegangsbeheer en autorisatie**	Wordt toegang tot persoonsgegevens beperkt tot wie deze nodig heeft?	Controle op functiescheiding, in- en uitdienstprocedures, periodieke controle van rechten.
C3	**Controle en evaluatie (toetsing, audits)**	Worden periodieke controles en evaluaties uitgevoerd en opgevolgd?	De FG of interne auditfunctie voert controles uit; opvolging en rapportage zijn aantoonbaar.
C4	**Meldplicht datalekken**	Worden datalekken tijdig gemeld en geregistreerd?	Toets op procedures, meldregistraties en leerpunten (AP-meldingen, interne meldingen).
D1	**Bewustwording en training**	Is personeel voldoende bewust en opgeleid over privacy en beveiliging?	Regelmatige trainingen, e-learning, communicatiecampagnes, toetsing van kennis.
D2	**Documentatie en verantwoording**	Worden verwerkingen, DPIA's en besluiten goed gedocumenteerd?	Denk aan het verwerkingsregister, rapportages aan bestuur, jaarlijkse FG-verslag.