WETTERSKIP FRYSLÂN

WATERSCHAPSBLAD

Officiële uitgave van het dagelijks bestuur van het Wetterskip Fryslân

Nr. 11529

21 september 2023

Beleidskader Privacy Wetterskip Fryslân

Het dagelijks bestuur van Wetterskip Fryslân heeft, gelezen het bestuursvoorstel op 13 juni 2023, vastgesteld het:

Beleidskader Privacy Wetterskip Fryslân

Het dagelijks bestuur heeft besloten om het beleidskader Privacy en de Wet Politiegegevens (WPG) vast te stellen. Hier is in verwoord op welke wijze we zorgvuldig en rechtmatig omgaan met persoonsgegevens, zodat de persoonlijke levenssfeer van betrokkenen, zoals inwoners en medewerkers, wordt gerespecteerd en dat op gepaste wijze gebruik wordt gemaakt van persoonsgegevens in de werkprocessen. De WPG is nadrukkelijker toegelicht.
Hiermee wordt de privacy van ingelanden en medewerkers gewaarborgd conform de AVG en de WPG.

1 Voorwoord

De samenleving is exclusief aangewezen op Wetterskip Fryslân voor schoon en voldoende water en voor veiligheid achter de dijken. Zij verwacht een hoge betrouwbare uitvoering van de aan ons toegewezen taken. Gelijktijdig wordt van Wetterskip Fryslân geacht, als overheidsorganisatie, zichtbaar, transparant, participerend en interactief te zijn met betrekking tot de uitvoering van onze taken tegen maatschappelijk aanvaardbare kosten.
Bij het uitvoeren van de wettelijke taken van Wetterskip Fryslân en in de interne organisatie is de verwerking van persoonsgegevens noodzakelijk. Het gaat daarbij onder andere om gegevens van inwoners en medewerkers.
Verregaande digitalisering van onze bedrijfsprocessen, de toenemende complexiteit, versterkte gegevensuitwisseling in ‘ketens’ van de overheid en samenwerkingspartners heeft tot gevolg dat extra aandacht nodig is voor de manier waarop we omgaan met persoonsgegevens.
Als overheidsorganisatie worden ook wij in de media en in de samenleving kritisch gevolgd en logischerwijs aangesproken op fouten wanneer er iets mis gaat met persoonsgegevens. Dit zorgt ook binnen het Wetterskip Fryslân voor een groeiende druk op de zorgvuldige omgang met persoonsgegevens.
Wetterskip Fryslân wil zorgvuldig met deze informatie om gaan, de privacy van de betrokkenen respecteren en voldoen aan wet- en regelgeving, zoals de AVG en WPG. Dit vraagt aandacht van alle medewerkers van bestuur tot uitvoering en inbedding in de werkwijze en processen van de organisatie. Om daarvoor te zorgen is dit beleid opgesteld.
Het Dagelijks Bestuur is integraal eindverantwoordelijk voor de manier waarop de organisatie omgaat met persoonsgegevens. Deze eindverantwoordelijkheid is gemandateerd aan de Secretaris-directeur.
Uiteindelijk hebben we allemaal een verantwoordelijkheid voor privacy. Onze organisatie is het meest effectief als privacy een integraal onderdeel is van het dagelijks handelen van alle medewerkers van het waterschap.
Het doel is om de kennis van privacy en de zorgvuldige omgang met persoonsgegevens te verankeren in de organisatie van het Wetterskip Fryslân.

2 Inleiding

2.1 Doel en functie beleidskader

Het doel van dit beleidskader privacy is het vaststellen en vastleggen van de doelstellingen en uitgangspunten met betrekking tot privacy, aangevuld met de manier waarop Wetterskip Fryslân dit wil realiseren. Hiermee vormt het beleid de leidraad voor de betrokkenen en geeft hiermee de interne organisatie en andere partijen duidelijkheid over de kaders waarbinnen de verwerkingen van persoonsgegevens op een rechtmatige wijze plaatsvinden.

2.2 Uitgangspunten Privacy

Het doel van privacy is de zorgvuldige en rechtmatige omgang met persoonsgegevens, zodat

- de persoonlijke levenssfeer van betrokkenen, zoals inwoners en medewerkers, wordt gerespecteerd,
- Wetterskip Fryslân op gepaste wijze gebruik maakt van persoonsgegevens in haar werkprocessen en
- Wetterskip Fryslân voldoet aan wet- en regelgeving.

Bij persoonsgegevens gaat het om alle gegevens die direct of indirect herleidbaar zijn naar natuurlijke personen. Ook gegevens gerelateerd aan autokentekens of netwerkadressen van computers of smartphones zijn daarmee persoonsgegevens.
Na de adoptie van de universele verklaring voor de rechten van de mens in 1948 zijn de uitgangspunten voor de bescherming van persoonsgegevens stap voor stap uitgewerkt, met name in Europees verband. Dit heeft geleid tot de volgende principes die in de AVG hun weerslag hebben gevonden die ook nagenoeg gelden voor de WPG:

- De verwerking van persoonsgegevens moet rechtmatig zijn, dat wil zeggen dat er een rechtmatige grondslag is, zoals toestemming, een wettelijke verplichting, de uitvoering van een wettelijke taak of een gerechtvaardigd belang.
- De verwerking van persoonsgegevens moet transparant zijn. Dat wil zeggen dat de betrokkenen zijn geïnformeerd over de verwerking van hun persoonsgegevens.
- Persoonsgegevens mogen alleen worden verwerkt voor een vooraf bepaald doel en mogen in de regel niet voor andere doelen worden gebruikt dan waarvoor ze zijn verzameld.
- Er mogen niet meer persoonsgegevens worden verwerkt dan voor het bepaalde doel noodzakelijk.
- Persoonsgegevens moeten juist en actueel zijn in relatie tot het doel waarvoor ze worden verwerkt.
- Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor het doel. In de context van Wetterskip Fryslân wordt deze termijn vaak bepaald door wettelijk voorgeschreven bewaartermijnen.
- De integriteit en vertrouwelijkheid van persoonsgegevens moeten worden beschermd door een passende informatiebeveiliging.
- Organisaties die persoonsgegevens verwerken moeten kunnen aantonen dat zij dit doen binnen de kaders van wet- en regelgeving.

Een groot deel van het gedachtegoed van de AVG en de typische AVG-producten zien we terug bij de WPG. Er worden daarnaast aanvullende eisen gesteld aan de bewaartermijnen, de verplichting tot logging, een aangepaste informatieplicht bij datalekken en een aangepaste rechtsbescherming van betrokkenen. Verder is er extra aandacht voor het gebruik van profiling en het benoemen van categorieën zoals verdachte, getuige, slachtoffer en overtreder.

2.3 Privacy en informatiebeveiliging

Er is een relatie tussen privacy en informatiebeveiliging aangezien de beveiliging van persoonsgegevens een in de vorige paragraaf genoemd principe is. Dit principe wordt vormgegeven in het Informatiebeveiligingsbeleid.
Daarom ligt het voor de hand dat privacy en informatiebeveiliging op een aantal gebieden samen optrekken, bijvoorbeeld bij:

- Inventarisatie van persoonsgegevens en dataclassificatie;
- Het bepalen van beveiligingseisen voor de verwerking van persoonsgegevens;
- Het afhandelen van incidenten en datalekken;
- Bewustwording en training van medewerkers;
- Het stellen van eisen aan nieuwe of gewijzigde systemen (privacy by design en default);

Op andere gebieden kan er ook een gezonde spanning zijn tussen privacy en informatiebeveiliging. Vanuit informatiebeveiliging kan de wens zijn om veel log-informatie te verzamelen, die terug te voeren is op gedrag van gebruikers. Tevens kan de wens zijn om deze gegevens zo lang mogelijk te bewaren. Vanuit privacy zal de wens zijn om zo min mogelijk gegevens te verzamelen en deze zo kort mogelijk te bewaren.

Bij de organisatorische inrichting van de rollen rond privacy en informatiebeveiliging binnen Wetterskip Fryslân is zowel rekening gehouden met de synergie als met de spanning tussen privacy en informatiebeveiliging. Binnen het waterschap zijn de rollen functionaris Gegevensbescherming en CISO (Chief Information Security Officer) belegd bij twee verschillende personen. Daar waar het Privacybeleid en het Informatiebeveiligingsbeleid raakvlakken hebben wordt gezamenlijk opgetrokken. Over initiatieven en projecten wordt vanuit beide invalshoeken geadviseerd en deze worden vanuit beide invalshoeken getoetst.
Binnen Wetterskip Fryslân wordt dit vergemakkelijkt doordat beide beleidsterreinen in het Security en Privacy Office zijn ondergebracht.

2.4 Eigenaarschap en onderhoud van dit document

Binnen het waterschap is het Dagelijks Bestuur integraal eindverantwoordelijk voor privacy. Het Dagelijks Bestuur heeft volgens het bestuursmodel deze verantwoordelijkheid gedelegeerd aan de Secretaris-directeur. Eigenaarschap van dit document ligt bij de Secretaris-directeur.

Dit document wordt periodiek op inhoud, uitvoerbaarheid, invoering en werking beoordeeld en, indien nodig, aangepast om te voorkomen dat het veroudert. Vanuit de directie wordt opdracht gegeven aan de Security en Privacy Office om de inhoudelijke evaluatie en bijstelling van dit beleid periodiek voor te bereiden en te agenderen.
Herziening van dit beleid is mede afhankelijk van de vormgeving van taken en werkprocessen binnen Wetterskip Fryslân, zoals een voortschrijdende digitalisering, wijzigingen in wet- en regelgeving, beleidsregels en uitspraken van toezichthouders, gerechtelijke uitspraken en de beheerorganisatie.
Het beleid wordt ten minste elke 3 jaar geëvalueerd en aangepast. Als er aanleiding voor is, wordt dit eerder gedaan.

3 Ambitie en kaders

Het privacybeleid met daarin het ambitieniveau is geen op zichzelf staand geheel. Het sluit aan op strategische beleidskaders, zowel binnen Wetterskip Fryslân als binnen de Nederlandse overheid. Het ambitieniveau en de kaders worden hier toegelicht.

3.1 Ambitieniveau

De ambitie ten aanzien van privacy is het zodanig uitvoeren van de wettelijke taken van Wetterskip Fryslân en gebruik van persoonsgegevens bij de interne organisatie dat er sprake is van een zorgvuldig en rechtmatig gebruik van persoonsgegevens. Dat betekent ook:

- Transparantie voor de burger en medewerker
- Goede inrichting binnen de organisatie
- Bewustwording en training voor medewerkers
- Inbedding in de P&C Cyclus, zodat we blijven voldoen
- Aantoonbaar maken dat we voldoen

In aansluiting met de kaders die de waterschappen hebben afgesproken, streeft Wetterskip Fryslân naar een goede beheersing. Dat wil zeggen dat risico's en eventuele tekortkomingen transparant zijn voor de directie. Op die manier kan de directie daarop bijsturen en gaat Wetterskip Fryslân aantoonbaar zorgvuldig en rechtmatig om met persoonsgegevens. Wetterskip Fryslân groeit daar al enkele jaren naar toe en zal daar de komende jaren naar toe blijven groeien.

3.2 Kaders Wetterskip Fryslân

Kaders komen uit het meerjarenbeleidsperspectief Wetterskip Fryslân 2018-2022 en de begrotin9 2018. De belangrijkste voor privacy worden hier benoemd:

- Een kernwaarde van het Wetterskip Fryslân is "kennis en kunde". Voor de uitvoering van genoemde kerntaken is de samenleving aangewezen op Wetterskip Fryslân; we kennen geen concurrentie. Dat stelt hoge eisen aan de betrouwbaarheid van ons werk; die moet gewoon goed zijn!
- Er is de laatste jaren fors ingezet op het denken en werken in processen. Het is nu zaak om door voortdurend verbeteren verder uit te bouwen. Het gedachtengoed van 'lean'-management biedt aanknopingspunten om dit te doen. Zaken soepel, vlot en vaardig laten verlopen, moet een tweede natuur worden. Dit raakt de AVG en de WPG omdat bij de beoordeling van de aanpassingen de aspecten van privacy moeten worden meegenomen (principe "Privacy by design")
- De organisatie maakt een ontwikkeling door naar een ketenorganisatie: overheid 3.0, wendbaar, slim en naar buiten gericht. Gekoppeld aan het gebiedsgericht werken en versterkt door een digitale transitie verwachten we optimalisaties in de keten te realiseren. Ook meer samenwerking tussen overheden zal bijdragen aan een klant- en doelgerichte overheid.

3.3 Kader Waterschappen

Volwassenheidsniveau

Waterschappen hebben in navolging van de Informatiebeveiliging afgesproken dat zij een bepaald volwassenheidsniveau voor privacy nastreven. In 2019[1] is in het CBCF bestuurlijk afgesproken dat de waterschappen toe groeien naar volwassenheidsniveau 4 op een schaal van 5[2]. Niveau 4 betekent volgens dit CMM-model [3]:

- het proces is volledig beheerst en een PDCA-cyclus is volledig in uitvoering;
- de inrichting van de organisatie en de processen is geïntegreerd;
- integratie in het gedrag, zoals in de voorbeeldfunctie van het management;
- monitoring op naleving en periodieke evaluatie van aanpak vindt plaats en
- zo nodig worden verbeteringen doorgevoerd en maatregelen getroffen op basis van een risicoanalyse.

Afgesproken is dat in 2022 de waterschappen voldoen aan het niveau 4[4]. In volwassenheidsniveau 4 wordt uitgegaan van een kwaliteitsbenadering. De PDCA (Plan Do Check Act) is hierbij volledig in de lijn geïmplementeerd en bescherming van persoonsgegevens wordt risico-gebaseerd en proactief opgepakt. Dat sluit, zoals de Autoriteit Persoonsgegevens heeft aangegeven, naadloos aan op de AVG waarin bepaald is dat "maatregelen geëvalueerd en indien nodig geactualiseerd dienen te worden."

Privacy baseline van het CIP
De AVG is een open norm. Om deze open norm verder in te vullen is "de Privacy baseline" als basis gebruikt bijvoorbeeld voor het opstellen van een landelijk programma Privacy. Dit is besloten door de opdrachtgevers voor het waterschaphuis. De opdrachtgevers (secretaris-directeuren) zijn de waterschappen zelf. Daarnaast is een voorstel over het gebruik van de baseline in 2017 naar het CBCF gegaan.

Het gebruik van deze baseline wordt nu weer prominenter opgepakt. Deze baseline wordt in 2021 gebruikt voor het uitvoeren van de landelijke toetsing en is het toetsingskader.
1) Moet nog formeel worden vastgesteld; dit is het advies van het UO aan de Unie
2) Voor informatiebeveiliging is hetzelfde niveau van toepassing
3) Capability Maturity Model
4) Beslisnota OGT over "Volwassenheidsniveau 4 voor privacybescherming met als doeljaar 2022" van 20 maart 2020

3.4 Kader Nederlandse overheid
Als waterschap hebben we contacten met andere Nederlandse overheden. De uitwisseling van persoonsgegevens met deze andere overheden is niet onbegrensd. Voor de uitwisseling van persoonsgegevens is telkens een rechtmatige grondslag nodig.
Daarnaast is de beveiliging van uit te wisselen gegevens randvoorwaardelijk. De Nederlandse overheden dienen allemaal te voldoen aan de Baseline Informatiebeveiliging Nederlandse Overheid. Daarom beschouwen we andere overheidsorganisaties als vertrouwde partner. Het gevolg hiervan is dat iedereen afzonderlijk zijn omgeving beveiligt en "schoon" houdt en dat de andere omgevingen hierop kunnen vertrouwen.

3.5 Kader Wet- en regelgeving
Het Wetterskip Fryslân hanteert de volgende voorschriften en wettelijke kaders voor privacy:
- Algemene Verordening Gegevensbescherming (AVG)
- Wet Politiegegevens (WPG) (voor strafrechtelijke taken, uitgevoerd door de Boa's)
- Telecomwet (met name ten aanzien van massamails en cookies op websites)
- Wet basisregistratie personen
- Kieswet
- Beleidsregels, aanwijzingen en adviezen van de Autoriteit persoonsgegevens (AP) en de European Data Protection Board (EDPB)
- Wet Open Overheid (WOO)
- Wet op de ondernemingsraden (WOR) (met name Art. 27 met betrekking tot verwerking van gegevens van medewerkers)
- Baseline Informatiebeveiliging Nederlandse Overheid (BIO), ten aanzien van informatiebeveiliging
- Archiefwet (t.a.v. bewaren en vernietigen van gegevens)

4 Zorgvuldige en rechtmatige organisatie

4.1 Inleiding
Wetterskip Fryslân stelt zich ten doel het zodanig uitvoeren van de wettelijke taken van Wetterskip Fryslân en het interne beheer dat er sprake is van een zorgvuldig en rechtmatig gebruik van persoonsgegevens.
Om dit te bereiken zijn de afgelopen jaren verbeteringen in de werkprocessen uitgevoerd, vooral rond de invoering van de AVG en de WPG. In de komende jaren is blijvende aandacht en doorontwikkeling nodig om:
- Vastgestelde en nieuw geïdentificeerde privacy risico's te minimaliseren.
- Privacy verder te verankeren in de werkwijze en processen binnen de organisatie.
- Rekening te houden met de veranderende organisatie van Wetterskip Fryslân.
- Rekening te houden met wijzigingen en aanscherping van wet- en regelgeving, beleidsregels van toezichthouders en gerechtelijke uitspraken.

De wijze waarop de zorgvuldigheid is georganiseerd wordt in de volgende paragrafen toegelicht.

4.2 Rollen en verantwoordelijkheden

Het Dagelijks Bestuur neemt door het vaststellen van het beleid haar verantwoordelijkheid om sturing te geven aan het thema privacy. Het algemeen bestuur stelt de hiervoor benodigde middelen beschikbaar. De (reguliere) P&C-cyclus met haar rapportages en jaarverslag informeert het dagelijks bestuur over het realiseren van het beleid. Daarnaast ontvangt het dagelijks bestuur jaarlijks een rapportage van de Functionaris Gegevensbescherming.

De directie heeft de verantwoordelijkheid om het beleid te realiseren. Binnen de organisatie is een opdrachtgever benoemd, die de specifieke verantwoordelijkheid draagt voor het onderwerp privacy. Op voorstel van de opdrachtgever Privacy gaat het beleid naar de directie. Over het realiseren van het beleid wordt periodiek aan de directie gerapporteerd.

De opgavemanagers zijn verantwoordelijk voor het bekend maken en het realiseren van het beleid. De opdrachtgever Privacy neemt de opgavemanagers mee in dit onderwerp zodat zij in gesprek kunnen gaan met hun vakgroepleiders, afspraken kunnen maken en de voortgang kunnen monitoren.

Conform het besturingsmodel van Wetterskip Fryslân zijn de vakgroepleiders in eerste lijn verantwoordelijk voor de omgang met persoonsgegevens en de borging van privacy. De vakgroepleiders leggen verantwoording af aan zijn opgavemanager (vakgroep). De vakgroepleiders zijn verantwoordelijk voor:

- het treffen van gepaste maatregelen op basis van risicomanagement;
- het inbedden van privacy in de werkprocessen;
- het actueel houden van het Register van verwerkingen;
- het uitvoeren van risicoanalyses (DPIA);
- het bevorderen van bewustwording;
- het benoemen en monitoren van verbeteracties (groeipaden);
- het laten zien dat de vakgroep aantoonbaar voldoet (toetsingen) .

Er is een handreiking in de vorm van een Privacygids opgesteld, die de vakgroepleider als extra toelichting kan gebruiken.

De Security en Privacy Office valt onder de vakgroep CFI en is belast met het geven van advies over en het monitoren van het voldoen aan de privacy-eisen vanuit de wetgeving en het beleid van Wetterskip Fryslân. Dit wordt gedaan door de privacy adviseurs en de Functionaris Gegevensbescherming. De privacy adviseur geeft advies en houdt de actualiteit van het verwerkingenregister bij. De rol van Functionaris Gegevensbescherming is door de AVG en de WPG voorgeschreven en richt zich op het houden van toezicht op de naleving van de AVG en de WPG, rapporteert hierover aan de directie en het bestuur en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens. Daarnaast worden er een aantal bewustwordingsactiviteiten georganiseerd.

Tenslotte wordt van de medewerkers verwacht dat zij verantwoordelijk zijn voor:

- zorgvuldige omgang met persoonsgegevens;
- geheimhouding van vertrouwelijke informatie;
- melden van verstoringen beveiligingsincidenten, bijna-incidenten, kwetsbaarheden en mogelijke dataleken .

De Autoriteit Persoonsgegevens (AP) ziet als extern toezichthouder toe op de naleving van de wettelijke verplichtingen.

4.3 Sturen en verantwoorden

Voor het effectueren van privacy wordt gewerkt via een Plan Do Check Act cyclus (zie onderstaande figuur).

Het rapporteren over privacy gebeurt met behulp van de bestaande verantwoordingslijnen. Daarnaast vindt er ieder jaar een jaarlijkse evaluatie en toetsingen plaats.

Bestaande verantwoordingslijnen
De basis voor het rapporteren begint bij de vakgroepen. Op basis van een evaluatie (het afgelopen jaar) en de ingeschatte risico's worden, waar nodig, groeipaden benoemd. De groeipaden gaan over de te nemen verbetermaatregelen. Verder geeft de vakgroep de werkzaamheden aan die nodig zijn om de basis op orde te houden en om aantoonbaar te voldoen. De groeipaden en genoemde werkzaamheden worden jaarlijks met de Security en Privacy office besproken, vastgelegd en ondertekend. Dit alles komt terecht in het plan Privacy (opdracht). De vakgroepleiders maken afspraken met hun opgavemanager (vakgroep) over het uit te voeren plan Privacy en de voortgang en regelen indien nodig de middelen. Belangrijke punten komen terug in het vakgroepplan, waarover periodiek aan de opgavemanager (vakgroep) wordt gerapporteerd.
Daarnaast maakt de Privacy Office een jaarplan Privacy voor de eigen werkzaamheden. Hierin staan de ondersteunende en toezichthoudende werkzaamheden.
Voor het overzicht op organisatieniveau wordt het jaarplan Privacy aangevuld met belangrijke gezamenlijke punten uit de plannen van de vakgroepen. Dit jaarplan Privacy wordt besproken met de opdrachtgever Privacy en de directie. De opdrachtgever Privacy bespreekt het jaarplan met de opgavemanagers. Het jaarplan en de aandachtspunten komen op hoofdlijnen terug in de opgave Privacy in het opgaveplan Bedrijfsvoering. De monitoring van deze opgave vindt op opgaveniveau plaats in de reguliere P&C-cyclus (opgaverapportage). De uitkomsten worden periodiek besproken met de directie en het bestuur.

4.4 Naleving en controle
Het waterschap heeft als verwerkingsverantwoordelijke de verplichting aan te tonen dat de verwerking van persoonsgegevens rechtmatig, behoorlijk en transparant heeft plaatsgevonden·. De FG brengt hierover ten minste jaarlijks verslag uit aan het Dagelijks Bestuur. Onderdeel van de aantoonbaarheid is het toetsen en het evalueren. Dit wordt hier vervolgens toegelicht.

Interne toetsingen (processen)
De vakgroepleiders zijn verantwoordelijk voor het aantoonbaar voldoen. Interne toetsingen op vakgroepniveau worden opgenomen in het plan op vakgroepniveau. De Privacy Office voert reviews uit op de interne toetsingen en zullen zelf een aantal toetsingen uitvoeren. De voortgang op de toetsingen wordt meegenomen in de voortgang op het plan op vakgroepniveau en het jaarplan Privacy. Daarnaast wordt een rapportage gemaakt waarin uitkomsten van de vakgroepen en de Privacy Office worden gebundeld zodat we inzichtelijke hebben waar we als organisatie staan. De voortgang komt in hoofdlijnen terug in de reguliere P&C-cyclus.

Jaarlijkse zelfevaluatie inrichting privacy
Jaarlijks wordt de inrichting van privacy binnen Wetterskip Fryslân geëvalueerd aan de hand van het Privacy Framework. De aandachtspunten in de baseline van het Centrum informatiebeveiliging en privacy (CIP) worden nader toegelicht in bijlage A. Daarnaast worden risico's geëvalueerd, o.a. op basis van de in het afgelopen jaar opgetreden datalekken, verzoeken van betrokkenen en andere relevante

gebeurtenissen. Deze evaluaties worden uitgevoerd met vertegenwoordigers uit de vakgroepen, met name de privacybeheerders. De resultaten worden meegenomen in de plannen op vakgroepniveau en het jaarplan Privacy van de Privacy Office. De uitkomsten worden jaarlijks gerapporteerd.

Beleidsevaluatie
De resultaten van de evaluaties worden ook in het licht van het beleid beoordeeld. Jaarlijks wordt een rapportage gemaakt over het realiseren van het beleid. Deze jaarlijkse rapportage wordt vastgesteld door de directie en het bestuur en wordt besproken door de opdrachtgever Privacy met de opgavemanagers.

WPG:
In de WPG is opgenomen dat het ieder jaar verplicht is om een interne en externe audit uit te voeren. De rapporten van de externe audit moeten worden gestuurd naar de Autoriteit Persoonsgegevens (AP). De AP geeft geen beoordeling op het niveau van een organisatie. Ze gebruiken de informatie uit de rapporten om bijvoorbeeld voorlichting te geven.

Aldus vastgesteld in de openbare vergadering van het dagelijks bestuur van 13 juni 2023,

L.M.B.C. Kroon,
Dijkgraaf
O. Bijlsma,
Secretaris-directeur

Bijlage A: Privacy Framework/jaarlijkse zelfevaluatie

Het borgen van de kwaliteit is verder uitgewerkt in een Privacy Framework. Dit Privacy Framework wordt gebruikt voor de jaarlijkse zelfevaluatie. Dit is naast de interne toetsingen een belangrijk instrument om te meten dat wij aantoonbaar voldoen aan de AVG. Ten aanzien van de WPG proberen we zo goed mogelijk aan te sluiten bij de werkwijze van de AVG. Waar mogelijk voegen we enkele passages toe aan de bestaande procedures en beleidsstukken. Als dit niet mogelijk is maken we afzonderlijke stukken. Het privacy framework is gebaseerd op "de privacy baseline" van het CIP (Centrum informatiebeveiliging en privacy). Aandachtsgebieden uit het framework worden hier kort toegelicht en daarna worden basis vereisten benoemd, die landelijk zijn aangegeven.

Deze aandachtspunten, zullen waar nodig, worden gebruikt in de jaarlijkse rapportage naar de directie en bestuur. Verder zullen deze aandachtspunten terug komen in de landelijke audits, die regelmatig plaatsvinden.

Algemeen

1. **Beleid**
   Het voorhanden zijn van privacy beleid en de implementatie daarvan, inclusief de plan-do-check-act cyclus.
2. **Organisatie**
   De vastlegging van verantwoordelijkheden voor het management, alle medewerkers en privacy-specifieke rollen, zoals die van de Functionaris Gegevensbescherming als intern toezichthouder , de vakgroepleider, vakgroepprivacybeheerder en privacy adviseur.
   Ook bewustwording en training vallen onder dit aandachtsgebied.
3. **Risicomanagement, privacy by design en de DPIA**
   De werkwijze rond nieuwe of gewijzigde verwerkingen, waaronder de borging van privacy by design en default, de uitvoering van Gegevensbeschermingseffectbeoordelingen (ook DPIA, Data Protection Impact Analysis genoemd) en de periodieke revisie daarvan. Indien nodig worden er naar aanleiding van de uitvoering van een DPIA passende technische en organisatorische beveiligingsmaatregelen getroffen, zoals bijvoorbeeld pseudonimisering van persoonsgegevens.

Verwerkingen van gegevens

4. **Verwerkingenregister (inclusief doelbinding en doorgifte persoonsgegevens)**
   Het opstellen en onderhouden van een overzicht van alle verwerkingen van persoonsgegevens in de organisatie. Het register gaat onder andere in op het doel van de verwerking, de rechtmatige grondslag, het verkrijgen en het verstrekken van gegevens.
5. **Gegevensbeheer (inclusief bewaren)**
   Maatregelen om de juistheid/actualiteit van gegevens te waarborgen en te zorgen dat gegevens niet langer worden bewaard dan noodzakelijk.
6. **Verwerkingen door / als verwerker**
   Het afsluiten van overeenkomsten met leveranciers die in opdracht van Wetterskip Fryslân persoonsgegevens verwerken, zoals leveranciers van ICT-diensten. Dit betreft ook de borging daarvan in bijvoorbeeld het inkoopproces en het afsluiten van overeenkomsten met organisaties in opdracht waarvan Wetterskip Fryslân persoonsgegevens verwerkt, zoals voor deelnemingen.
7. **Informatiebeveiliging**
   De mate waarin er sprake is van een passende informatiebeveiliging, bij Wetterskip Fryslân gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO).

Transparantie

8. **Informeren van betrokkenen**
   Het informeren van alle groepen betrokkenen over de verwerking van hun persoonsgegevens, bijvoorbeeld door het geven van toelichting over privacy in de brieven (privacy verklaringen voor medewerkers, bestuurders en inwoners) en bezoekers van de website.
9. **Rechten van betrokkenen**
   De organisatie van de afhandeling van verzoeken van betrokkenen wanneer zij een beroep doen op de rechten die hen zijn toegekend in de AVG.

Beheersing

10. **Rechtmatigheid van de verwerking**
    De periodieke evaluatie van de rechtmatigheid van de verwerking van persoonsgegevens, gelet op de principes die in paragraaf 2.2 zijn genoemd.
11. **Meldplicht datalekken**
    De organisatie van de afhandeling van datalekken.

Basisvereisten HWH (landelijk niveau)

Al voor de invoering van de AVG in mei 2018 heeft Het Waterschapshuis een aantal basisvereisten opgesteld. Deze zijn en worden gebruikt om de voortgang van de implementatie van de AVG landelijk te monitoren. Het gaat om de volgende onderwerpen:

- Aanstellen van een FG
- Instellen van een Privacydesk/toetsteam (facultatief)
- Bewustwordingsactiviteiten
- Rol van de FG
- Register van verwerkingsactiviteiten
- Rechten van betrokkene
- Processen verzoeken betrokkene
- Privacy beleid
- Extern privacy statement
- Model DPIA
- Beschrijving uitvoering DPIA
- Proces datalek
- Registratie en rapportage van privacy incidenten
- Model verwerkersovereenkomsten
- Classificatie van persoonsgegevens (facultatief) *)

*) Deze wordt meegenomen bij informatiebeveiliging. In de BIO staan gerichte controls benoemd.