FG-jaarrapportage 2022

Gemeente Zwartewaterland

CLASSIFICATIE:	Geheim
VERSIE:	1.2
DATUM:	6 april 2023

Inhoudsopgave

1 Documentbeheer

Documenteigenschappen

Titel	FG-jaarrapportage 2022
Onderwerp	Jaarrapportage 2022 Functionaris Gegevensbescherming
Auteur	[functionaris gegevensbescherming]
Documenttype	
Classificatie	Geheim
Eigenaar	Functionaris Gegevensbescherming

Versiebeheer

Versie	Datum	Auteur	Review	Aard van aanpassing
0.1	25-01-2023	L2P	N.v.t.	Initiële opzet
0.2	13-02-2023	L2P	PO, CISO, Controller	Feedback verwerkt
1.0	13-02-2023	L2P		Definitieve versie
1.1	06-03-2023	L2P		Classificatie aangepast
1.2	06-04-2023	L2P		Kleine inhoudelijke wijziging doorgevoerd nav overleg in het college

2 Managementsamenvatting

2.1 Naleving

De gemeente Zwartewaterland (hierna: gemeente) heeft in 2018 een aantal maatregelen getroffen om aan de Algemene Verordening Gegevensbescherming (hierna: AVG) te voldoen. Door beperkte personele capaciteit, een focus op de afhandeling van ad hoc privacyvraagstukken en minder aandacht voor governance en procesmatig werken, zijn sindsdien achterstanden ontstaan. Dit betekent dat de gemeente anno 2022 onvoldoende in controle is op het gebied van privacy. Daarmee voldoet de gemeente niet volledig aan de AVG.

Privacy moet onderdeel worden van de dagelijkse bedrijfsvoering daarnaast, moet de Plan-Do-Check-Act (PDCA) op worden gezet. Dat is geen gemakkelijke opgave, de FG constateert dat veel gemeenten moeite hebben met het verhogen van het volwassenheidsniveau. Een belangrijk onderdeel is dat privacy aan de voorkant wordt geborgd, bijvoorbeeld: bij inkoop, projectmanagement en wetswijzigingen. Commitment vanuit de gehele organisatie is belangrijk om deze doelen te halen.

De Functionaris Gegevensbescherming is door de gemeente aangesteld als interne toezichthouder voor de Wet politiegegevens (hierna: Wpg) en voor de AVG. Vanwege de recente Wpg-audit heeft ten behoeve van dit rapport geen nieuwe toetsing van Wpg-naleving plaatsgevonden.

De voornaamste bevindingen en aanbevelingen van de FG voor de AVG zijn:

Bevinding	**Actie**
Er is geen formeel vastgesteld privacybeleid met een rapportagecyclus.	Stel een organisatiebreed privacybeleid op en vast en richt een rapportagecyclus in.
De privacyverklaring is onvolledig en het inzageproces is niet vastgelegd.	Update de privacyverklaring en richt een procedure in voor de opvolging van verzoeken van betrokkenen voor de uitoefening van hun rechten.
Er is nog geen procedure ingericht voor DPIA's en pre-DPIA's.	Richt een formeel proces in voor het tijdig bepalen van doelbinding en wettelijke grondslag (pre-DPIA) en voor het uitvoeren van een DPIA.
Achterstand implementatie verbetermaatregelen Wpg-audit.	Stel een verbeterplan op n.a.v. de externe audit en zorg voor voldoende interne capaciteit hiervoor.

2.2 Verzoeken en bezwaren, klachten

Er zijn in 2022 geen AVG-verzoeken door betrokkenen gedaan.

2.3 Datalekken

In 2022 zijn twee datalekken gemeld binnen de organisatie. Het aantal datalekken is hiermee ten opzichte van 2021 gelijk gebleven. In 2022 zijn er geen datalekken gemeld bij de Autoriteit Persoonsgegevens (hierna: AP) net zoals in 2021. Eén datalek is gemeld aan betrokkenen. Beide datalekken zijn veroorzaakt door verkeerd geadresseerde brieven of e-mails. Voor een uitgebreider overzicht van de datalekken wordt verwezen naar Bijlage II.

2.4 Data protection impact assessments (DPIA's)

De AVG schrijft voor om, voorafgaand aan een nieuwe verwerking met een mogelijk hoog risico voor de betrokkenen, een zogenaamd *data protection impact assessment* of gegevensbeschermingseffectbeoordeling (GBE)(hierna: DPIA) uit te voeren waarmee gestructureerd de voorgenomen verwerking, de daarmee gepaard gaande risico's en benodigde maatregelen in kaart worden gebracht.

In 2022 zijn twee DPIAs uitgevoerd en twee DPIA's gestart. Voor een uitgebreid overzicht van de uitgevoerde DPIA's wordt verwezen naar Bijlage III.

2.5 Planning en activiteiten

De samenwerking tussen privacy, informatiebeveiliging en interne audit wordt de komende periode verder versterkt door middel van structureel periodiek overleg tussen de drie onderdelen en waar mogelijk een gezamenlijke visie en/of rapportage

Samen met informatiebeveiliging zal worden gewerkt aan een gemeentebrede bewustwordingscampagne voor medewerkers .

De privacy officer (hierna: PO) is in het vierde kwartaal van 2022 gestart met het opstellen van het privacybeleid. De oplevering hiervan volgt in 2023.

De PO coördineert medio 2023 de update van het verwerkingsregister. Daarnaast wordt een procedure voor DPIA's opgezet en de bijbehorende documentatie verbeterd.

De FG heeft in het vierde kwartaal van 2022 de organisatie getoetst op het bestaan van de noodzakelijke privacybeheersmaatregelen. De FG zal in 2023 bijzondere aandacht besteden aan risicomanagement, leveranciersmanagement en de rechten van betrokkenen.

3 Inleiding

In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de gemeente transparant te zijn welke persoonsgegevens zijn verwerkt en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. Ook moet de gemeente passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoonsgegevens te voorkomen. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen.

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Op deze verwerkingen vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dient de organisatie te beschikken over een interne toezichthouder: de Functionaris voor de Gegevensbescherming (FG).

De FG ziet erop toe dat de AVG intern wordt nageleefd. Voor gemeente Zwartewaterland is L2P ingehuurd als FG. De gemeente Zwartewaterland heeft de opdracht erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door hem toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan, en hem de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in stand houden van zijn deskundigheid. De uitvoerende taken liggen bij de privacy officer (PO).

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden, bevindingen en aanbevelingen. Dit jaarverslag is bedoeld voor de burgemeester en het college van B&W. De gemeenteraad zal als zelfstandige verwerkingsverantwoordelijke en als controlerend orgaan van het college van B&W separaat een verslag ontvangen.

3.1 Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken naar het jaar 2022. Wat heeft gemeente Zwartewaterland bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG? In het tweede deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2023 naar een hoger niveau te tillen en in lijn te brengen met de wettelijke eisen. Hierbij wordt waar nodig tevens aandacht geschonken aan de technische en organisatorische maatregelingen die nodig zijn om dit hogere niveau te bereiken en te voldoen aan de AVG.

In dit rapport worden veertien privacy thema's genoemd. Dertien thema's zijn afkomstig uit het Privacy Baseline model van het Centrum Informatiebeveiliging en Privacybescherming (CIP). Het veertiende thema is de Wet politiegegevens (Wpg). In de volgende paragrafen volgt een korte toelichting op alle privacy thema's.

3.1.1 CIP Privacy Baseline model

Het CIP heeft de Privacy Baseline ontwikkeld met als doel organisaties duidelijkheid te geven over wat, waar, door wie en op welke wijze zij zaken moet regelen om privacy op de juiste wijze te waarborgen. Het CIP heeft de eisen van de AVG en UAVG vertaald naar concrete, hanteerbare normen die duidelijk maken wat organisaties moeten doen om in overeenstemming met de wet de privacy van de betrokkenen te waarborgen. In bijlage 1 is per thema beknopt weergegeven in hoeverre de gemeente de normen reeds heeft geïmplementeerd. In het eerste deel van de rapportage (Hoofdstuk 4) wordt de stand van zaken in 2022 per thema toegelicht.

Er worden dertien thema's verdeeld over drie domeinen onderscheiden:

a. Het Beleidsdomein bestaande uit de thema's Privacybeleid (1), Organisatie (2) en Risicomanagement (3).
b. Het Uitvoeringsdomein bestaande uit de thema's Doelbinding (4), Register van verwerkingen (5), Kwaliteitsmanagement (6), Beveiliging (7), Informatieverstrekking (8), Bewaren (9) en Doorgifte (10).
c. Het Control- en Beheerdomein bestaande uit de thema's Toezicht (11), Rechten van Betrokkenen (12) en Meldplicht datalekken (13).

3.1.2 Wet politiegegevens

De Wet politiegegevens (Wpg) verplicht gemeenten, als werkgever van buitengewoon opsporingsambtenaren (boa's), om een FG aan te stellen voor het interne toezicht op de Wpg. De huidige FG voor de AVG is door de gemeente tevens aangesteld als interne toezichthouder op de Wpg. Om die reden is in deze rapportage het thema Wpg toegevoegd als extra thema naast de dertien privacy thema's uit de AVG. De gemeente is verplicht om iedere vier jaar een externe audit uit te laten voeren. Daarnaast is de gemeente verplicht om jaarlijks een interne audit uit te voeren. De bevindingen van de FG omtrent de uitvoering van de Wpg door de gemeente worden onder dit thema beschreven (zie paragraaf 4.14).

4 Deel 1. Terugblik op 2022

In dit hoofdstuk wordt beschreven op welke wijze Zwartewaterland invulling heeft gegeven aan de privacy thema's. Iedere paragraaf begint met een korte omschrijving van de norm en wordt gevolgd door een beschrijving van de aangetroffen situatie en de getroffen maatregelen in 2022.

4.1 Privacybeleid

Het privacybeleid is een kader waarin de gemeente aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe de gemeente omgaat met persoonsgegevens en op welke wijze invulling wordt gegeven aan de wettelijke beginselen.

Binnen de gemeente Zwartewaterland is er geen privacybeleid opgesteld. Aan een aantal wettelijke verplichtingen zoals het registreren en melden van datalekken en het borgen van de rechten van betrokkenen is praktisch invulling gegeven door middel van procedures. Deze procedures functioneren in de praktijk maar zijn nog niet formeel vastgesteld als beleidsdocument. In september 2022 is de PO-functie structureel ingevuld. De PO heeft onder andere de taak gekregen om het privacybeleid en de procedures (verder) te ontwikkelen en te beheren.

4.2 Organisatie

Het doel van een heldere verdeling van taken en bevoegdheden, van middelen en rapportagelijnen is waarborgen dat op de juiste wijze invulling wordt gegeven aan de eisen van het privacybeleid en de AVG. Daarnaast omvat het thema Organisatie ook de bewustwording op de vloer van het bestaan van privacy, de privacyregels en hoe dit intern is georganiseerd.

Er is nog geen volledige privacy-organisatie ingericht. De taken, bevoegdheden en verantwoordelijkheden (TBV) zijn op het gebied van privacy nog niet vastgesteld. In het Informatiebeveiligingsbeleid 2019-2023 is een TBV-matrix vastgesteld voor de relevante functies op het gebied van informatiebeveiliging. Deze verdeling van taken, bevoegdheden en verantwoordelijkheden kan als voorbeeld dienen voor de privacy functies.

Het onderwerp privacy staat nog niet voldoende op de agenda van de directie. Periodiek wordt de stand van zaken met betrekking tot informatiebeveiliging door de Chief Information Security Officer (hierna: CISO) met de gemeentesecretaris besproken. Het thema privacy wordt op ad-hoc basis door het Management Team (hierna: MT) besproken, echter een formele rapportagecyclus voor de PO en de CISO richting het MT is nog niet ingericht.

De gemeente heeft voorts aandacht voor het onderwerp bewustwording en voldoende budget voor het organiseren van bewustwordingsactiviteiten. Medewerkers zijn zich bewust van het belang van privacy en van de bescherming van persoonsgegevens en overige vertrouwelijke informatie. Iedere medewerker wordt via de VNG getoetst op kennis over informatiebewustzijn. De eenheidsmanagers zijn verantwoordelijk voor de functie specifieke bewustwording. Er zijn in 2022 activiteiten georganiseerd om het privacy bewustzijn te verbeteren en te onderhouden. Hierbij wordt nog niet volgens een algemeen bewustwordingsprogramma voor privacy gewerkt.

4.3 Risicomanagement, Privacy by design en Privacy by default

Voor effectief risicomanagement is een beoordeling door de gemeente van de privacy risico's (de kans en hun potentiële omvang/impact) nodig om te bepalen hoe deze risico's, door het treffen van maatregelen, teruggebracht kunnen worden tot binnen de grenzen die de gemeente acceptabel acht. De gemeente dient daarnaast passende technische en organisatorische maatregelen te nemen om de waarborgen van de AVG in de verwerking in te bouwen. De beoordeling van de privacy risico's (de kans en hun potentiële omvang/impact) is nodig om te bepalen hoe deze, door het treffen van maatregelen, teruggebracht kunnen worden tot binnen grenzen die de organisatie acceptabel acht.

De gemeente weegt privacy risico's ad hoc mee en indien wettelijk verplicht worden deze risico's aan de hand van een DPIA in kaart gebracht voor nieuwe of gewijzigde verwerkingen. De gemeente beschikt sinds eind 2022 over een DPIA-format. Een bijbehorende methodiek voor de uitvoering van een DPIA heeft de gemeente nog niet geïmplementeerd.

Voor de uitvoering van verplichte DPIA's hanteert de gemeente nog geen centrale planning. De gemeente Zwartewaterland is in 2022 onder begeleiding van L2P gestart met de uitvoering van vier DPIA's. Hiervan zijn er intussen twee afgerond en met een advies van de FG aangeboden aan de verantwoordelijk manager. De rapportage en monitoring van de opvolging van de risico mitigerende maatregelen uit deze DPIA's heeft nog geen vorm gekregen.

Privacy by design wordt deels toegepast, met name bij de inrichting van nieuwe projecten. Iedere manager is verantwoordelijk voor de inrichting van privacy by design, waaronder de uitvoering van DPIA's en privacy by default (de standaard instelling van producten en diensten met de hoogste mate van privacy).

Voorts is de gemeente in transitie naar een actieve professionele werkwijze op het gebied van projecten, waarbinnen ook de onderwerpen privacy en informatiebeveiliging de aandacht krijgen. Het eigenaarschap is op het niveau van processen reeds vastgelegd. Er bestaat binnen de gemeente een groot draagvlak voor het doorvoeren van verbeteringen.

4.4 Doelbinding

De gemeente dient de doeleinden en de rechtvaardigingsgronden van alle verzamelingen en verwerkingen van persoonsgegevens tijdig, welbepaald en uitdrukkelijk te omschrijven.

Doelbinding is essentieel om persoonsgegevens te mogen verwerken. Voor het gebruik van persoonsgegevens van burgers zijn doeleinden en rechtvaardigingsgronden in kaart gebracht en opgenomen in de online privacyverklaring. In de privacyverklaring is tevens aandacht besteed aan cookies. De privacyverklaring is opgesteld in 2019 en tussentijds niet geüpdatet. De gemeente heeft nog geen proces ingericht dat waarborgt dat zij doelbinding en wettelijke grondslag tijdig (voorafgaand aan de verwerking) vastlegt en beoordeelt.

4.5 Register van verwerkingen

De gemeente dient als verwerkingsverantwoordelijke, en in voorkomende gevallen als verwerker, de gegevens over de gegevensverwerkingen vast te hebben gelegd in een register van verwerkingen. Dit register dient een actueel en samenhangend beeld te bieden van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.

De gemeente heeft een verwerkingsregister waarin de doeleinden en rechtvaardigingsgronden van de verwerkingen zijn vastgelegd. Dit verwerkingsregister is op dit moment niet actueel vanwege het ontbreken van beheer. Hierdoor heeft de gemeente geen volledig inzicht in haar verwerkingen van persoonsgegevens, het verband tussen verwerkingen, processen, organisatie en systemen. De PO is in het vierde kwartaal van 2022 gestart met de inrichting van het beheer van het verwerkingsregister.

4.6 Kwaliteitsmanagement

De gemeente dient kwaliteitsmanagement te hebben ingericht ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking dient zo te zijn ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt of overgedragen. Als dit op verzoek van betrokkene gebeurt dient deze over de status van de afhandeling te worden geïnformeerd.

Via de privacyverklaring informeert de gemeente de betrokkenen over o.a. het inzagerecht. In de privacyverklaring worden niet alle rechten van betrokkenen genoemd. De gemeente hanteert een werkwijze voor de afhandeling van verzoeken van betrokkenen omtrent hun rechten zoals het inzagerecht. Verzoeken kunnen door betrokkenen worden ingediend via de gemeentelijke website en ingekomen verzoeken worden door de CISO of de PO afgehandeld. Deze werkwijze is nog niet formeel vastgelegd.

4.7 Beveiliging

Elke organisatie die persoonsgegevens verwerkt dient passende technische en organisatorische maatregelen te nemen om de veiligheid van de persoonsgegevens te waarborgen. De gemeente dient in dit kader te borgen dat zij alsmede haar verwerkers, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.

De gemeente beschikt over een informatiebeveiligingsbeleid dat is opgesteld in 2019. Dit beleid is geldig voor de periode 2019-2023 en wordt geüpdatet bij de introductie van de vernieuwde Baseline Informatiebeveiliging Overheid (BIO 2.0) in 2023.

Een onderdeel van het informatiebeveiligingsbeleid is het beheer van hardware. Hiervoor is een procedure ingericht, waarbij wordt geregistreerd wie gebruik maakt van welke apparatuur en wanneer deze apparatuur ingeleverd dient te worden. Hiermee kan de gemeente monitoren waar hun apparatuur zich bevindt en wanneer deze apparatuur ingeleverd dient te worden, bijvoorbeeld bij uitdiensttreding. Ook is er invulling gegeven aan het ‘bring your own device’ principe, waardoor medewerkers hun eigen apparatuur veilig kunnen gebruiken voor hun werkzaamheden voor de gemeente. Er is op het gebied van informatiebeveiliging nog geen sluitend systeem van leveranciersmanagement vanwege het ontbreken van een periodieke controle op de naleving van de (contractuele) beveiligingseisen bij uitbestede verwerkingen.

4.8 Informatieverstrekking

De verwerkingsverantwoordelijke dient bij elke verzameling van persoonsgegevens tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar te stellen, om een behoorlijke en transparante verwerking te waarborgen. De gemeente dient in dit kader passende maatregelen te hebben genomen om transparante informatie te communiceren met de betrokkenen.

De gemeente heeft een privacyverklaring via haar website gepubliceerd. Hierin wordt nog geen onderscheid gemaakt tussen de verschillende categorieën betrokkenen zoals inwoners, medewerkers, zakelijke contactpersonen, bezoekers van de website etc. Daarnaast zijn niet alle rechten van betrokkenen afgedekt in de privacyverklaring. De noodzakelijke update van de privacyverklaring wordt onder leiding van de PO in 2023 uitgevoerd.

4.9 Bewaren

De gemeente dient de nodige maatregelen te treffen om ervoor te zorgen dat bewaartermijnen niet worden overschreden.

De Selectielijst gemeenten en intergemeentelijke organen 2020 wordt hiervoor door de gemeente gehanteerd. Aan de hand van deze selectielijst controleert de gemeente per procestype welke bewaartermijn geldt, en is op deze manier in staat om gegevens tijdig te verwijderen. Een organisatiebreed beleid is nog niet aanwezig.

4.10 Doorgifte

Bij doorgifte door de gemeente aan een andere verwerkingsverantwoordelijke dienen de onderlinge verantwoordelijkheden duidelijk te zijn en bij de doorgifte aan een verwerker dienen er afdoende garanties te zijn. Daarnaast gelden er aanvullende eisen bij de doorgifte naar landen buiten de Europese Unie (EU), te weten:

- er is een vertegenwoordiger, en;
- er is geen sprake van uitzonderingsgronden en;
- er geldt een door de Europese Commissie genomen adequaatheidsbesluit, of;
- er zijn er passende waarborgen, of;
- er geldt een afwijking voor een specifieke situatie.

De gemeente Zwartewaterland controleert periodiek de diensten van leveranciers. Dit wordt door het Shared Service Centrum ONS (hierna: ONS) beheerd. De gemeente stelt de eisen vast en de naleving hiervan wordt door ONS gecontroleerd. De gemeente maakt nauwelijks gebruik van doorgifte naar andere landen, en in het bijzonder landen buiten de EU. Een volledig overzicht van de verwerkingslocaties bij doorgifte ontbreekt op dit moment.

4.11 Toezicht

De gemeente is als overheidsorgaan door de AVG verplicht om een FG aan te stellen. Daarnaast is de aanstelling van een FG verplicht onder de Wet politiegegevens (Wpg). Voorts dient de gemeente in het kader van haar verantwoordingsplicht, als één van de beginselen inzake de verwerking van persoonsgegeven, de rechtmatigheid van haar gegevensverwerkingen te evalueren en aan te kunnen tonen.

De FG-functie is sinds de uitdiensttreding van de FG per 1 september 2021 waargenomen door een gedeelde FG van de gemeenten Meppel, Staphorst, Steenwijkerland, Westerveld en Zwartewaterland. Medio 2022 hebben deze vijf gemeenten zich laten adviseren over de verdere invulling van de rol van de FG.[1] In september 2022 is de samenwerking tussen de gemeenten voor de FG-rol beëindigd en vult L2P de functie van FG voor de gemeente Zwartewaterland in.

Er wordt door risico-eigenaren nog niet periodiek gerapporteerd over de effectiviteit van de maatregelen en over privacy risico's op eigen niveau. Corrigerende acties worden nog niet genomen volgens een Plan-Do-Check-Act-cyclus (hierna: PDCA-cyclus). De PDCA-cyclus is een

[1] Zie Adviesrapport invulling FG 0.91 van L2P d.d. 7 juli 2022.

gangbare methode om invulling te geven aan de verantwoordingsplicht en wordt tevens gehanteerd binnen een Information Security Management System (ISMS).

4.12 Rechten van betrokkenen

De gemeente dient iedere betrokkene informatie over de verwerking van persoonsgegevens te bieden en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen, tenzij er een specifieke uitzonderingsgrond geldt. Het gaat hier om het waarborgen van de rechten van een betrokkene op inzage, rectificatie, vergetelheid, overdraagbaarheid en bezwaar.

Betrokkenen worden via de privacyverklaring geïnformeerd over bepaalde rechten, echter dekt deze verklaring niet alle rechten af. Voor de opvolging van verzoeken van betrokkenen omtrent hun rechten is nog geen formule procedure opgesteld en vastgesteld. In de huidige werkwijze zijn verder geen tekortkomingen geconstateerd.

4.13 Meldplicht datalekken

De gemeente dient een datalek binnen 72 uur aan de AP te melden, de inbreuk te documenteren en de betrokkene(n) te informeren. Tenzij hiervoor een uitzondering geldt.

De gemeente heeft een formele, uitgeschreven datalekprocedure en deze wordt periodiek onder de aandacht gebracht van alle medewerkers via intranet. Ieder vermoeden van een datalek wordt gemeld aan de PO en de PO is verantwoordelijk voor de registratie van een datalek. Indien van toepassing worden de datalekken door L2P aan de Autoriteit Persoonsgegevens gemeld. Medewerkers zijn op de hoogte van de geldende procedure, maar niet ieder (potentieel) datalek wordt als zodanig herkend.

4.14 Wet politiegegevens (Wpg)

Conform de Wpg dient de gemeente, als werkgever van buitengewoon opsporingsambtenaren (boa's), twee jaar na inwerkingtreding van de Wpg (op 1 januari 2022) en vervolgens eenmaal per vier jaren een externe privacy audit uit te voeren. Hoewel de vierjaarlijkse externe audit in 2021 uitgevoerd moest worden, heeft de AP een jaar uitstel gegeven. De gemeente Zwartewaterland heeft de externe audit over 2022 in 2022 voor het eerst uit laten voeren. Ter voorbereiding op deze externe audit wordt jaarlijks een interne audit uitgevoerd welke is te vergelijken met een zelfevaluatie. De interne audit (opzet, bestaan en werking) heeft betrekking op enkele onderdelen van de Wpg en heeft tot doel voor de onderdelen van de wet waar de interne audit zich op richt, op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven.

In 2022 heeft de gemeente een externe audit over 2021 uit laten voeren. Deze audit is afgerond met een rapportage met daarin een aantal verbetervoorstellen. Het adviesbureau BMC heeft van de gemeente de opdracht gekregen om een plan van aanpak (PvA) op te stellen voor de implementatie van de voorgestelde verbetermaatregelen. De oplevering van het PvA is vertraagd wegens een gebrek aan de benodigde interne capaciteit bij de gemeente. De interne audit over 2022 heeft de gemeente niet uitgevoerd in 2022.

4.15 Conclusie

Er is door de gemeente nog veel werk te verzetten om de AVG verder te implementeren in de organisatie, de systemen en de processen.

Een aantal maatregelen blijken effectief. Zo is de afgelopen jaren een begin gemaakt met de implementatie van de AVG en door het in 2022 samengestelde team Informatiemanagement is het mogelijk om de aanwezige basis verder uit te bouwen. Met de huidige samenstelling van het team Informatiemanagement is namelijk voldoende algemene privacy kennis en capaciteit aanwezig om de privacyvraagstukken van de gemeente op te kunnen pakken en de AVG verder te implementeren.

Daarnaast is gebleken dat de procedure voor het melden van datalekken qua opzet gedegen is. De procedure waarborgt dat beveiligingsincidenten kunnen worden gemeld, tijdig worden beoordeeld en indien sprake is van een datalek wordt dit, indien verplicht, tevens tijdig gemeld bij de AP.

Er zijn ook een aantal aandachtspunten voor de gemeente om aantoonbaar te kunnen voldoen aan de AVG. In het tweede deel van deze rapportage zullen aanbevelingen worden gedaan om gegevensbescherming daadwerkelijk in te bedden in de gemeentelijke organisatie.

5 Deel 2. Vooruitkijken naar 2023

Gegevensbescherming onderdeel laten zijn van de processen en systemen van het college, en daarmee aantoonbaar voldoen aan privacywetgeving, is een continu proces. Het vraagt om structurele borging van dit onderwerp. Het jaar 2022 heeft in het teken gestaan van een structurele en adequate invulling van de PO-functie en van de FG-functie ten behoeve van de verdere implementatie van de AVG. Deze implementatie en benodigde verbeteringen zullen in 2023 centraal staan.

Hierna volgt een overzicht van de aanbevelingen van de FG voor de te nemen beheersmaatregelen per thema om privacy volwassenheidsniveau 3 (vastgesteld) te bereiken.

5.1 Privacybeleid

Aanbevelingen:

1. Stel op organisatieniveau formeel een eenduidig privacybeleid en procedures op, op zodanige wijze dat het duidelijk is welke (privacy) beheersmaatregelen de gemeente implementeert om haar privacy principes te waarborgen. In de uitwerking moet duidelijk zijn wie wat doet, wanneer en hoe.
2. Stel beleid en procedures voor de diverse afdelingen op in lijn met het beleid op organisatieniveau.

5.2 Organisatie

Aanbevelingen:

3. Richt een privacy organisatie in. Zorg dat duidelijk is wie intern verantwoordelijk is voor een verwerking en risicoanalyse (DPIA) en leg dit vast. De taken, bevoegdheden en verantwoordelijkheden van zowel privacy functies (PO, Information Security Officer (ISO), FG en privacy contactpersonen (bijv. “Privacy Champions”) als privacy taken van de lijnorganisatie worden duidelijk weergegeven in een helder overzicht (TBV/RASCI-matrix).
4. Borg dat risico-eigenaren periodiek rapporteren over de effectiviteit van de maatregelen en privacy risico’s op eigen niveau. Bespreek deze en neem waar nodig corrigerende acties volgens een PDCA-cyclus.
5. Stel vast hoe het huidige privacy bewustzijn is op management- en afdelingsniveau. Stel vervolgens op basis van de resultaten een bewustwordingsprogramma op waarmee alle managers en werknemers aantoonbaar generieke privacy en security kennis opdoen. Borg dat per doelgroep aantoonbare specifieke verdieping van de AVG, de UAVG en gemeentelijke privacy principes kan worden opgedaan.

6. Zorg dat het thema privacy structureel op de agenda van het MT komt te staan. Hierbij is het ook van belang dat een formele rapportagecyclus wordt ingericht, zodat er een directe lijn tussen de privacy organisatie en het MT wordt ingericht.

5.3 Risicomanagement, Privacy by design en Privacy by default

Aanbevelingen:

7. Stel (mede) op basis van deze rapportage de privacy risico's voor de gemeente vast en de noodzakelijke acties om de risico's te mitigeren.
8. Werk in de nog op te stellen procedures de privacy by design en – default aspecten uit zodat risico-, proces-, contract-, applicatie- en /of systeem-eigenaren in het geval van nieuwe of gewijzigde programma's, processen of applicaties, het privacy aspect aantoonbaar beoordeeld wordt voorafgaand aan de uitvoering van (nieuwe) verwerkingen.
9. Implementeer organisatie breed een DPIA-methodiek waarbij de voornoemde eigenaren weten wanneer zij verplicht een DPIA moeten uitvoeren. Laat periodiek monitoren en rapporteren dat dit ook daadwerkelijk gebeurt (bijvoorbeeld door een PO).
10. Stel een centrale DPIA-planning op om de achterstanden met betrekking tot de verplichte DPIA's in te halen en monitor de uitvoering hiervan.

5.4 Doelbinding

Aanbevelingen:

11. Onderzoek of de privacyverklaring overeenkomt met de huidige verwerkingen en pas deze zo nodig aan.
12. Borg dat op afdelingsniveau en organisatie breed tijdig (voor aanvang van gewijzigde of nieuwe verwerkingen) het doel en de wettelijke grondslag is bepaald en beoordeeld.

5.5 Register van verwerkingen

Aanbevelingen:

13. Onderzoek of het verwerkingsregister overeenkomt met de huidige situatie en pas deze aan.
14. Maak één of meerdere medewerkers verantwoordelijk voor het beheer van het verwerkingsregister en stel dit vast in het (nieuwe) privacybeleid.
15. Maak de interne procesverantwoordelijken verantwoordelijk voor de juistheid en de volledigheid van de aan te leveren gegevens voor het verwerkingsregister.

16. Stel een procedure op die waarborgt dat de gemeente het verwerkingsregister tijdig bij gewijzigde of nieuwe verwerkingen update. Borg in diezelfde procedure dat de interne procesverantwoordelijken periodiek monitoren of hun verwerkingen nog actueel, volledig en juist zijn en inzicht geven in de samenhang tussen de verwerkingen, processen, applicaties, systemen en derde partijen.

5.6 Kwaliteitsmanagement

Aanbevelingen:

17. Werk een organisatiebrede procedure met een werkinstructie uit zodat deze waarborgt dat de gemeente alle verzoeken van betrokkenen conform de wettelijke vereisten uitvoert en dat zij de verzoeken tijdig afhandelt. De volgende rechten dienen in deze procedure en werkinstructie te worden geborgd:
    i. inzage;
    ii. vergetelheid (gegevenswissing);
    iii. rectificatie en aanvulling
    iv. dataportabiliteit
    v. beperking van de verwerking;
    vi. menselijke blik bij besluitvorming (geautomatiseerde besluitvorming) indien van toepassing;
    vii. bezwaar; en
    viii. informatie.
18. Pas de privacyverklaring aan zodat deze informatie biedt over alle rechten van betrokkenen.

5.7 Beveiliging

Aanbevelingen:

19. Bewaak de effectiviteit van de informatiebeveiligingsmaatregelen op een formeel vastgestelde manier op uitvoerings-afdelings-en organisatieniveau, zodat elk persoonsgegeven aantoonbaar adequaat is beveiligd.
20. Borg in het nieuwe informatiebeveiligingsbeleid een ISMS met PDCA-cyclus.
21. Draag zorg voor voldoende middelen om een implementatie van een volledige PDCA-cyclus realiseren, zodat de gemeente op basis van effectiviteit (die o.a. gemeten kan worden door audits, monitoring en pen-testing), gebruikservaring en incidenten het ISMS aantoonbaar continue verbetert.
22. Borg dat uitbestede verwerkingen (bijv. via een shared service centrum (SCC)) adequaat en aantoonbaar zijn beveiligd en controleer dit periodiek.

5.8 Informatieverstrekking

Aanbeveling:

23. Waarborg dat de gemeente de betrokkenen (inwoners, werknemers (vast en inhuur), zakelijke contactpersonen, bezoekers website etc.) adequaat, tijdig en aantoonbaar informeert. Dit kan met behulp van een of meerdere privacyverklaringen.

5.9 Bewaren

Aanbeveling:

24. Stel organisatiebreed beleid op, bijv. in de vorm van een bewaartermijnenreglement, waaruit blijkt wie verantwoordelijk is voor het bepalen van de termijnen, hoe de bewaartermijnen nageleefd moeten worden, hoe en aan welke eisen tijdige vernietiging van persoonsgegevens dient plaats te vinden en wie zorgt voor monitoring op de naleving.

5.10 Doorgifte

Aanbevelingen:

25. Laat, na de update van het verwerkingsregister, contracteigenaren vaststellen of voor alle uitbestede verwerkingen een verwerkersovereenkomst, onderlinge regeling of een gegevensuitwisselingsovereenkomst aanwezig is.
26. Identificeer alle relevante risico's voor de uitbestede verwerkingen en beoordeel of de risico's voldoende gemitigeerd zijn.
27. Waarborg in het beleid voor outsourcing dat de contracteigenaar minimaal jaarlijks vaststelt of de afspraken uit de verwerkersovereenkomst, onderlinge regeling of een gegevensuitwisselingsovereenkomst o.a. op het gebied van beveiliging worden nageleefd.

5.11 Toezicht

Aanbeveling: zie aanbeveling 4 in paragraaf 5.2 Organisatie).

5.12 Rechten van betrokkenen

Aanbevelingen: zie aanbevelingen 16 en 17 in paragraaf 5.6 Kwaliteitsmanagement.

5.13 Meldplicht datalekken

Aanbeveling:

28. Borg in het outsourcing-beleid dat waar verplicht een verwerkersovereenkomst wordt gesloten.

5.14 Wet politiegegevens (Wpg)

Aanbeveling:

29. Draag er zorg voor dat de betrokken medewerkers voldoende tijd hebben voor de uitvoering van de Wpg.
30. Stel een plan van aanpak op voor de interne audit over 2022 en voer deze zo snel mogelijk uit.

5.15 Conclusie

Op het gebied van privacy en gegevensbescherming is er in 2023 winst te behalen. Met name de thema's Organisatie, Risicomanagement en Beveiliging verdienen komend jaar extra aandacht.

In Bijlage 1 is per privacy thema een samenvattend beeld geschetst van de beoordeling ten aanzien van de omgang met persoonsgegevens binnen de gemeente Zwartewaterland. Bij deze beoordeling wordt ook een inschatting gegeven van het volwassenheidsniveau van de geïmplementeerde maatregelen binnen een thema. Hiervoor hanteert het CIP een schaalverdeling met 5 niveaus. Deze schaalverdeling is gebaseerd op wereldwijde best practices en geeft zodoende een geharmoniseerd beeld en de mogelijkheid tot het benchmarken met andere organisaties.

De schaalverdeling ziet er als volgt uit:

1. Informeel: de privacy werkzaamheden worden op verwerkingsniveau informeel uitgevoerd.
2. Beheerst: de privacy werkzaamheden worden beheerst uitgevoerd (herhaalbare processen).
3. Vastgesteld: de privacy werkzaamheden worden binnen de organisatie volgens een vastgestelde werkwijze uitgevoerd.
4. Voorspelbaar: de privacy prestaties worden gemeten, vergeleken met de branche en gebruikt voor een optimaal lerend vermogen.
5. Geoptimaliseerd: uitingen ten aanzien van de prestaties maken optimaal (integraal) onderdeel uit van de bedrijfsstrategie en -uitingen.

Artikel 5 lid 2 jo artikel 24 lid 1 AVG verplicht organisaties (verwerkingsverantwoordelijke) aantoonbaar te voldoen aan de voorwaarden van de AVG ('verantwoordingsplicht'). Dit betekent dat op basis van het bovenstaand volwassenheidsmodel een

verwerkingsverantwoordelijke uiteindelijk minimaal niveau 4 (’aantoonbaar compliant’) dient te behalen om voldoende zekerheid te hebben over het naleven van de privacyregelgeving. In dit rapport zijn de aanbevolen maatregelen gefocust op het bereiken van niveau ‘vastgesteld’ gecombineerd met de implementatie van een Plan Do Check Act (PDCA) cyclus tot op directieniveau waarmee de organisatie na gemiddeld een jaar, het niveau ‘voorspelbaar’ kan aantonen.

Bijlage I Stand van zaken AVG per thema

Thema	Volwassenheid	Risico
Privacybeleid Binnen de gemeente Zwartewaterland is er geen formeel privacybeleid vastgesteld.		
Organisatie Er is sprake van privacy bewustzijn binnen de gemeente, privacy staat nog niet standaard op de agenda van het management. Taken en verantwoordelijkheden op het gebied van privacy zijn niet vastgesteld.		
Risicomanagement, privacy by design, privacy by default De gemeente hanteert voor DPIA's een DPIA-format. Een DPIA-procedure ontbreekt. Privacy by design wordt deels toegepast, voornamelijk bij de inrichting van nieuwe processen.		
Doelbinding Er is geen formeel proces ingericht voor het tijdig bepalen van doelbinding en wettelijke grondslag.		
Register van verwerkingen Er is een register van verwerkingen, maar dit register is op dit moment niet up-to-date vanwege het ontbreken van beheer. De PO is recent gestart met de inrichting van het beheer van het verwerkingsregister.		
Kwaliteitsmanagement Via de privacyverklaring worden betrokkenen geïnformeerd over hun rechten. Echter is deze privacyverklaring niet volledig en is het inzageproces niet formeel ingericht.		
Beveiliging De gemeente beschikt over een actueel informatiebeveiligingsbeleid. Ook is er invulling gegeven aan het beheer van hardware, en het 'bring-your-own-device' principe.		
Informatieverstrekking De gemeente beschikt over een privacyverklaring, deze is niet actueel en zal in 2023 worden geüpdatet. Ook bevat deze privacyverklaring niet alle rechten van betrokkenen.		
Bewaren De gemeente hanteert voor het bepalen van de bewaringstermijn de selectielijst van de VNG.		

Thema	Volwassenheid	Risico
Doorgifte De gemeente controleert periodiek de diensten van leveranciers. Een volledig overzicht van verwerkingslocaties ontbreekt op dit moment.		
Toezicht Risico-eigenaren rapporteren nog niet periodiek over de effectiviteit van de maatregelen en privacy risico's op eigen niveau. Ook is er nog geen formele implementatie van een Plan-Do-Check-Act cyclus ingericht.		
Rechten van betrokkenen De rechten van betrokkenen zijn verwerkt in de privacyverklaring, maar deze is niet volledig. Ook is er geen formele procedure voor verzoeken van betrokkenen.		
Meldplicht datalekken De gemeente beschikt over een formele datalekkenprocedure. Medewerkers zijn op de hoogte van deze procedure, en wat te doen in het geval van een datalek. Leveranciers worden niet periodiek gecontroleerd.		
Wet Politiegegevens De gemeente heeft een externe audit laten uitvoeren over het naleven van de Wet Politiegegevens. Hieruit zijn verbetermaatregelen gekomen en is een plan van aanpak opgesteld.		

Bijlage II Overzicht datalekken

Datalek	Gemeld aan AP	Gemeld aan betrokkenen	Mitigerende maatregelen
Verkeerd geadresseerde email	Nee	Nee	Verkeerde ontvanger gevraagd de mail te wissen, met excuses. In het vervolg nauwgezette controleren of het mailadres klopt.
Verkeerde bijlage aan de mail toegevoegd	Nee	Ja	Beter letten op het toevoegen van de juiste bijlage. Bij herhaling mogelijk verdere acties.

Bijlage III Overzicht uitgevoerde DPIA's

Onderwerp DPIA	Datum	Status
Migratie jeugdwet naar de applicatie Suites voor het sociale domein.	14-11-2022	Afgerond
Vroegsignalering schulden	12-12-2022	Afgerond
Registratie arbeidsmigranten	08-06-2022	In behandeling
Wet inburgering	02-05-2022	In behandeling

L2P B.V.
Postbus 648
6800 AP Arnhem

+31 (0) 26 848 3118
info@L2P.nl