Waterschap Rivierenland

WATERSCHAPSBLAD

Officiële uitgave van het dagelijks bestuur van het Waterschap Rivierenland

Nr. 17447

21 juli 2025

Privacybeleid Waterschap Rivierenland 2025

Het college van dijkgraaf en heemraden van Waterschap Rivierenland;

Op voordracht van de directieraad van 16 december 2024;

Overwegingen:

Waterschap Rivierenland (WSRL) verwerkt persoonsgegevens en politiegegevens bij de uitvoering van wettelijke taken en dienstverlening. WSRL hecht veel waarde aan zorgvuldige, integere, publieke dienstverlening. Dit betekent dat betrokkenen erop moeten kunnen vertrouwen dat WSRL zich aan de wet houdt en gegevens zorgvuldig, rechtmatig, transparant en veilig verwerkt.

Het privacybeleid is van toepassing op de hele organisatie, alle taken en processen, objecten, gegevensverzamelingen en onderliggende informatiesystemen waar WSRL verantwoordelijk voor is.

In vergelijking tot het privacybeleid 2022 dat “de opzet en het bestaan” van privacy binnen WSRL beschrijft, gaat het privacybeleid 2025 verder in op “de werking en de beheersing” van privacy binnen de organisatie. Hiermee voldoet WSRL aan de vereiste documentatieplicht om een volgend volwassenheidsniveau 4 te kunnen realiseren. Het privacybeleid gaat in op de rollen en verantwoordelijkheden bij beleidsvorming, planning en uitvoering. Bestuur en management spelen een cruciale rol in het actief volgen en uitdragen van dit privacybeleid. Het privacybeleid dient ervoor om op bestuurlijk en ambtelijk niveau duidelijkheid te geven over de inrichtingskeuzes van privacy om te groeien naar een volgend volwassenheidsniveau.

Uit dit beleid volgt hoe door WSRL dagelijks met privacy wordt omgegaan en wat wettelijk verantwoord is. Bestuur en management spelen een cruciale rol in het actief volgen en uitdragen van dit privacybeleid. Het beleid is gebaseerd op relevante Europese en nationale en wet- en regelgeving.

Wettelijk kader:

- De Algemene verordening gegevensbescherming (AVG)
- De Uitvoeringswet algemene verordening gegevensbescherming (UAVG)
- De Wet politiegegevens

BESLUIT:

Vast te stellen het Privacybeleid Waterschap Rivierenland 2025

Artikel 1. Beleidsregel

1. Vast te stellen Privacybeleid Waterschap Rivierenland 2025, opgenomen als bijlage 1 bij dit besluit.
2. Bij deze beleidsregel behoren de volgende bijlagen:
   a. Bijlage 1 Begrippen;
   b. Bijlage 2 CIP Privacy Baseline criteria

Artikel 2. Intrekking

Privacybeleid Waterschap Rivierenland 2022, vastgesteld bij besluit van 21 juni 2022, wordt ingetrokken.

Artikel 3. Inwerkingtreding

Deze beleidsregel treedt in werking met ingang van de eerste dag na bekendmaking in het Waterschapsblad .

Artikel 5. Citeertitel

Deze beleidsregel wordt aangehaald als: Privacybeleid Waterschap Rivierenland 2025.

1. Inleidend summary

Het Waterschap Rivierenland te Tiel (WSRL), verwerkt persoonsgegevens bij de uitvoering van wettelijke taken en de uitvoering van zijn publiekrechtelijke taken. WSRL hecht veel waarde aan zorgvuldige,

integere, publieke dienstverlening. Dit betekent dat betrokkenen (de personen waarvan de gegevens worden verwerkt). erop moeten kunnen vertrouwen dat WSRL zich aan de wet houdt en gegevens zorgvuldig, rechtmatig, transparant en veilig verwerkt.

Het privacybeleid is van toepassing op de gehele organisatie, op alle taken en processen, objecten, gegevensverzamelingen en onderliggende informatiesystemen waar WSRL verantwoordelijk voor is.

In vergelijking tot het privacybeleid 2022 dat "de opzet en het bestaan" van privacy binnen WSRL beschrijft, gaat het privacybeleid 2025 verder in op "de werking en de beheersing" van privacy binnen de organisatie. Hiermee voldoet WSRL aan de vereiste documentatieplicht om een volgend volwassenheidsniveau 4 te kunnen realiseren.

Het privacybeleid gaat in op de rollen en verantwoordelijkheden bij beleidsvorming, planning en uitvoering. Bestuur en management spelen een cruciale rol in het actief volgen en uitdragen van dit privacybeleid. Het privacybeleid dient ervoor om op bestuurlijk en ambtelijk niveau duidelijkheid te geven over de inrichtingskeuzes van privacy om te groeien naar een volgend volwassenheidsniveau.

Uit dit beleid volgt hoe door WSRL dagelijks met privacy wordt omgegaan en wat wettelijk verantwoord is. Bestuur en management spelen een cruciale rol in het actief volgen en uitdragen van dit privacybeleid. Het beleid is gebaseerd op relevante Europese en nationale en wet- en regelgeving.

WSRL verwerkt persoonsgegevens volgens de volgende basisprincipes:
- WSRL verwerkt persoonsgegevens conform de eisen van de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg);
- WSRL verwerkt de noodzakelijke persoonsgegevens ter uitvoering van haar dienstverlening, ter bescherming van haar eigendommen en ter uitvoering van wettelijke en publieke taken;
- WSRL verwerkt de noodzakelijke persoonsgegevens van medewerkers ter uitvoering van haar taken en bevoegdheden als werkgever;
- WSRL zorgt ervoor dat de verkregen persoonsgegevens overeenkomen met de doelstellingen waarvoor deze worden verwerkt;
- WSRL hanteert bij het verwerken van persoonsgegevens de principes Privacy by Design en Privacy by Default.
- WSRL hanteert de uitgangspunten van de 'CIP Privacy Baseline'.
- In de verdeling van taken, rollen en verantwoordelijkheden wordt het principe van het 'Three Lines Model' gevolgd.

Het privacy beleid is vastgesteld en beoordeeld binnen de organisatie. Het bevat de visie op en de principes waarlangs privacy binnen de organisatie wordt georganiseerd. Het beleid wordt periodiek of bij relevante, significante wijzigingen van wet- en regelgeving beoordeeld op toepasselijkheid op de meest recente ontwikkelingen.

2. Algemeen

Aanleiding, Privacy Visie en Ambitieniveau

Aanleiding

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) rechtstreeks van toepassing in alle lidstaten van de Europese Unie. De AVG beschermt enerzijds de positie van de betrokkenen. Anderzijds legt de AVG-verplichtingen op aan WSRL, als organisatie die persoonsgegevens verwerkt. Eén van die verplichtingen is het vaststellen van privacybeleid.

Het verwerken van persoonsgegevens is geen kernactiviteit van WSRL, maar een afgeleide van of ondersteunend aan de primaire processen. In dat verband werkt iedere medewerker van WSRL in meer of mindere mate met persoonsgegevens. De persoonsgegevens hebben betrekking op enerzijds gegevens van burgers en anderzijds op gegevens van collega's en derde partijen (waaronder ook worden verstaan persoonsgegevens van bedrijven en organisaties waarmee het waterschap samenwerkt).

Met het vaststellen van privacybeleid wil WSRL in-control zijn voor wat betreft het omgaan met persoonsgegevens. Naast een goede beveiliging en verantwoord gebruik van persoonsgegevens, waarbij wordt voldaan aan wet- en regelgeving, worden privacyrisico's geïnventariseerd en worden passende maatregelen genomen. In het privacybeleid geeft WSRL op organisatorisch- en strategisch niveau duidelijkheid over de keuze van de inrichting van privacy om te waarborgen dat de verwerking op een rechtmatige wijze plaatsvindt. Daarmee voldoet WSRL aan de in de AVG en Wpg opgenomen verantwoordingsplicht.

Privacy Visie

"Als overheidsorganisatie heeft Waterschap Rivierenland wettelijk taken waarvoor het noodzakelijk is om persoonsgegevens te verwerken. Op ons rust een belangrijke verantwoordelijkheid om zorgvuldig om te gaan met deze persoonsgegevens, zowel van de inwoners van ons werkgebied als van onze collega's, zowel medewerkers als bestuurders. Daarbij houden we ons vanzelfsprekend aan de wet. Maar naast de wettelijke bepalingen laten we ook ethiek meewegen in onze keuzes. Het vertrouwen van onze betrokkenen is een groot goed en mag niet geschaad worden door onrechtmatige, onjuiste of onzorgvuldige verwerking van persoonsgegevens."

Ambitieniveau

In november 2019 is de opdrachtgeverstafel van de Unie van Waterschappen akkoord gegaan met het Programmaplan Informatieveiligheid en Privacy 2020-2024 (versie 0.8), waarin de ambitie is vastgelegd om de AVG in "opzet en bestaan" per 1 januari 2022 aantoonbaar te hebben geïntegreerd in de bedrijfsvoering van de waterschappen (volwassenheidsniveau 3).

Op 15 mei 2020 heeft de Commissie Bestuurszaken, Communicatie en Financiën (CBCF) van de Unie van Waterschappen besloten de ambitie van het volwassenheidsniveau voor privacy voor alle waterschappen vast te stellen op 4. Dit om 'de werking en beheersing" van de implementatie van de AVG in de bedrijfsvoering van de waterschappen aantoonbaar te maken. Voor het bepalen van de volwassenheid van (persoons-)gegevensbescherming binnen Waterschap Rivierenland gebruiken we het Capability Maturity Model (CMM). Dit is een model dat aangeeft op welk niveau de volwassenheid van de organisatie zit en wat ook wordt gebruikt voor andere processen.

Nu binnen WSRL de privacy beheersmaatregelen gedocumenteerd zijn (volwassenheidsniveau 3,2), is het van belang om te blijven sturen en te prioriteren om de groei naar volwassenheidsniveau 4 te realiseren. Met de invoering van privacy plannen sinds 2023 is een belangrijke eerste borging van planmatige en voortdurende verbetering (PDCA-cyclus) tot stand gekomen. Privacy plannen en het privacybeleid dienen verder geïntegreerd te worden in de operationele procedures en de dagelijkse praktijk. Verbetering van gedocumenteerde procedures zal leiden tot een effectievere controle en sturing van het gehele privacy proces. Dit vastgestelde privacybeleid levert een belangrijke bijdrage om volwassenheidsniveau 4 te kunnen bereiken.

Risico

Kwaliteit

Niveau Volwassenheid	Omschrijving
1. Initieel	Reactief, als er iets binnenkomt of gebeurt, dan wordt er op gereageerd (of niet...).
2. Herhaalbaar	Sturing en uitvoering van standaard werk vindt op een afgesproken wijze plaats. Verbetering verloopt projectmatig, sommige uitvoerende activiteiten verlopen ook projectmatig.
3. Gedefinieerd	Vastgelegde, beschreven en/of met tools ondersteunde processen die samenwerken en afstemmen waar dat nodig is (over afdelingen heen).
4. Beheerst	Een PDCA (Plan Do Check Act) die volledig in de lijn is geïmplementeerd en waarbij de beveiliging van (persoons)gegevens risico-gebaseerd en proactief wordt opgepakt. Dat wil zeggen: het management is in control en stuurt erop dat kwaliteit van informatieveiligheid en privacy wordt gemeten en zo nodig verbeterd (check - act). Informatieveiligheid en privacy is een integrale bestuurs- en directieaangelegenheid.
5. Geoptimaliseerd	Continu kijken of het beter kan, lerende organisatie Hierna wordt voor de volwassenheidsniveaus 2, 3 en 4 aangegeven wat het niveau betekent ten aanzien van de "monitoring, de onderbouwing, de mensen en de inrichting en structuur".

3.2 Status

>4.0 Ambitie

Doelen van het Privacybeleid

Dit privacybeleid dient ervoor om op organisatie- en strategisch niveau duidelijkheid te geven over de inrichtingskeuzes van privacy en te waarborgen dat de verwerking van gegevens op een rechtmatige wijze plaatsvindt.

<u>Kwaliteit en veiligheid</u>

Het privacybeleid heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren, waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

<u>Positionering van WSRL als betrouwbaar Waterschap</u>

Daarnaast geeft het privacybeleid medewerkers en andere betrokkenen inzicht in de wijze waarop WSRL omgaat met privacy. Het privacybeleid helpt bij het creëren van bewustwording over het belang en de noodzaak van het verantwoord omgaan met en het beschermen van persoonsgegevens. Als gevolg daarvan kunnen betrokkenen erop vertrouwen dat WSRL op een zorgvuldige en betrouwbare manier omgaat met persoonsgegevens.

Bewustwording
Het privacybeleid is dan ook van belang voor alle medewerkers, betrokkenen en organisaties waarmee WSRL samenwerkt. Het privacybeleid heeft consequenties voor het werk van alle medewerkers die met persoonsgegevens werken. Het privacybeleid heeft betrekking op het verwerken van persoonsgegevens en wordt, bij aanvang van de werkzaamheden met hen gedeeld, waarbij ook wordt ingegaan op de vraag wat dit beleid voor de werkzaamheden betekent.

Transparantie in rollen en verantwoordelijkheden
Vanuit de wettelijke en dienstverlenende taken heeft WSRL te maken met het verwerken van persoonsgegevens van betrokkenen binnen het waterschap, waaronder alle bestuursleden, medewerkers, bezoekers en externe relaties. In dit verband kan onder andere worden gedacht aan het verlenen van vergunningen, de personeelsadministratie en het behandelen van bezwaren, klachten en aansprakelijkstellingen. Door toenemende samenwerking met (overheids-)partners neemt de ketenverwerking van persoonsgegevens toe. Het is daarom belangrijk inzicht te hebben waar persoonsgegevens zich in de organisatie bevinden en wie verantwoordelijk is voor de verwerking ervan.

Respect voor betrokkene(n)
Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens, die betrekking hebben op een betrokkene, dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik en tegen verlies of misbruik op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij WSRL.

Wettelijk kader
WSRL is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het privacybeleid. Voor het privacybeleid gelden onder andere de volgende wettelijke kaders:
- De Algemene verordening gegevensbescherming (AVG)
- De Uitvoeringswet algemene verordening gegevensbescherming (UAVG)
- De Wet politiegegevens (Wpg)

In de Europese Economische Ruimte (EER) is de AVG van toepassing. De ruimte die de AVG laat om nadere invulling op nationaal niveau te geven, is ingevuld door de UAVG. De AVG legt een verantwoordingsplicht aan organisaties op die persoonsgegevens verwerken om aantoonbaar te maken dat zij voldoen aan de regels op het gebied van persoonsgegevensbescherming. WSRL verwerkt persoonsgegevens en moet aantonen:
1) *welke gegevensverwerkingen plaatsvinden;*
2) *dat de verwerkingen aan de belangrijkste beginselen van gegevensverwerking voldoen o.a. rechtmatigheid, transparantie, doelbinding en juistheid en*
3) *dat er technische en organisatorische maatregelen zijn genomen om persoonsgegevens te beschermen (laatste stand der techniek).*

De Wpg is een Nederlandse wet die regels stelt voor de verwerking van politiegegevens. Bij het opsporen van strafbare (milieu)feiten verwerken de buitengewoon opsporingsambtenaren van afdeling VTH van WSRL persoonsgegevens. Het verwerken van persoonsgegevens voor het uitvoeren van de politietaak (politiegegevens) valt onder de Wet politiegegevens (Wpg). De Wpg heeft een eigen, maar met de AVG vergelijkbaar beschermings- en verantwoordingsregime.

Als bestuursorgaan is WSRL gebonden aan de algemene regels van de Algemene wet bestuursrecht (Awb) en ook gebonden aan de regels die voortvloeien uit onder andere de Waterwet, de Waterschapswet en het Waterschapsbesluit. Regels rondom het bewaren en vernietigen van persoonsgegevens volgen uit de Archiefwet en de Selectielijst Waterschappen. Verder zijn nog de volgende (wettelijke) kaders van belang:
- Baseline Informatiebeveiliging Overheid (BIO)
  De BIO is een set van richtlijnen en maatregelen die zijn ontworpen om de informatiebeveiliging binnen de Nederlandse overheid te waarborgen.
- De Europese AI Act (AI Act):
  Op 21 mei 2024 heeft de Europese Raad goedkeuring gegeven aan de AI Act. De AI Act is een Europese verordening die richtlijnen vaststelt voor autonoom opererende computersystemen en algoritmen die beslissingen nemen, inhoud genereren of mensen ondersteunen. Het doel is om

ervoor te zorgen dat mensen en organisaties in de EU kunnen vertrouwen op veilige, transparante, niet-discriminerende en milieuvriendelijke AI-systemen. De verordening hanteert een risico gebaseerde benadering en legt verplichtingen op aan aanbieders en gebruikers, afhankelijk van het risiconiveau van het AI-systeem. Het Waterschapshuis ondersteunt WSRL mede om te komen tot adequate richtlijnen voor de inzet hiervan.

In diverse bijzondere wetten, die ook voor het WSRL relevant zijn, zijn ook regels met betrekking tot privacy opgenomen. Zo bevatten o.a. de Telecommunicatiewet, de Algemene wet inzake rijksbelastingen, het Wetboek van Strafrecht en de Wet basisregistratie personen afwijkende en/of aanvullende eisen ten aanzien van de privacy.

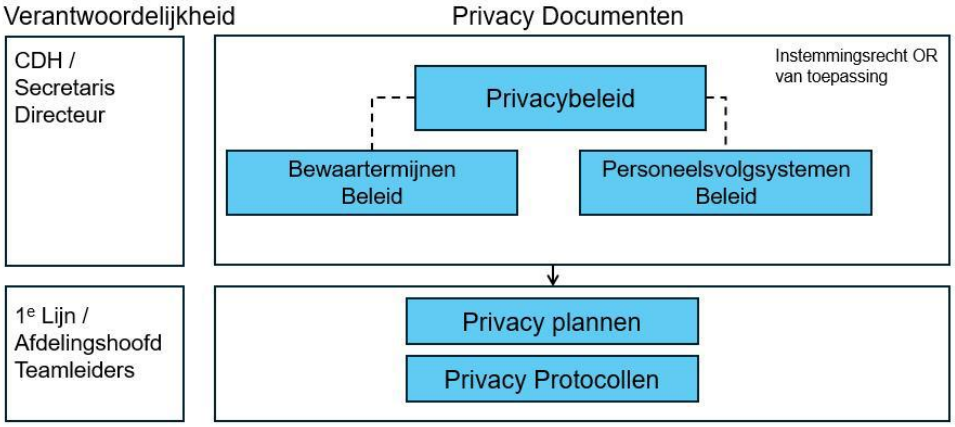
De betreffende bijzondere wetten dienen in onderlinge samenhang met de AVG te worden bezien. Over het algemeen geldt als uitgangspunt dat de AVG van toepassing is als algemene wet, waarvan de bepalingen echter niet van toepassing zijn indien er bijzondere wetgeving geldt.

Reikwijdte privacybeleid

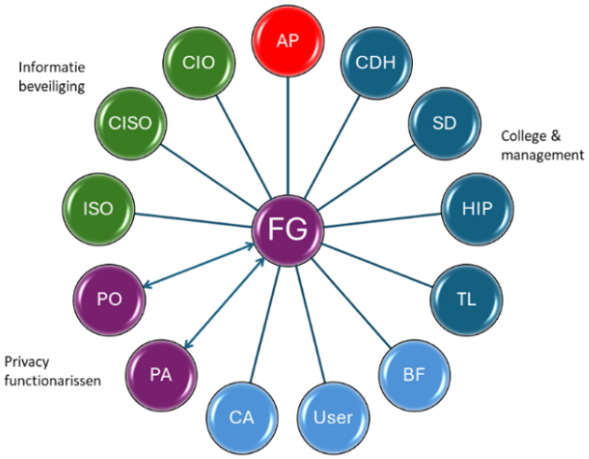
Privacy is een breed begrip om het (grond)recht op de persoonlijke levenssfeer van een individu te beschrijven. Daaronder vallen niet alleen persoonsgegevens, maar ook fysieke en sociale aspecten. Dit beleid richt zich in eerste instantie op de informationele privacy, omdat de privacywetgeving zich daar op richt. Informationele privacy betekent bescherming van personen in verband met de informatie die over hen bekend is en ten aanzien van hen wordt toegepast.

Het privacybeleid is van toepassing op de gehele organisatie, op alle taken en processen, objecten, gegevensverzamelingen en onderliggende informatiesystemen waar WSRL verantwoordelijk voor is. Bij de implementatie van dit geactualiseerde beleid zullen de proceseigenaren, procesmanagers en medewerkers van WSRL worden betrokken.

Hiervoor zijn binnen WSRL de volgende documenten en verantwoordelijkheden van toepassing.



Stakeholders binnen privacy:



AP	Autoriteit Persoonsgegevens
FG	Functionaris Gegevensbescherming
CDH	College van Dijkgraven en Heemraden
SD	Secretaris Directeur
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ISO	Information Security Officer
HIP	Afdelingshoofden
TL	Teamleiders
PO	Privacy Officers
PA	Privacy Ambassadeurs
Users	Medewerkers en externe gebruikers
BG	Bevoegde Functionarissen (Wpg)
CA	Communicatie Adviseur

Ten aanzien van belastinggegevens gelden de bepalingen van de Algemene wet inzake rijksbelastingen (AWR). Tevens dient bij belastinggegevens rekening te worden gehouden met de omstandigheid dat de heffing en de inning door WSRL slechts is beperkt tot de leges.

De overige waterschapsbelastingen worden namelijk op basis van delegatie opgelegd en geïnd door Belastingsamenwerking WSRL (BSR, een gemeenschappelijke regeling met een openbaar lichaam), waarvan WSRL één van de deelnemers is. Door deze delegatie zijn alle bevoegdheden en verplichtingen aangaande de overgedragen waterschapsbelastingen overgegaan op BSR, zodat BSR voor dit deel zelfstandig verantwoordelijk is voor het naleven van de AVG en de fiscale wetgeving inzake privacy en geheimhouding.

Dit privacybeleid gaat niet in op fysieke beveiliging en informatieveiligheid binnen WSRL. Een aantal beleidstukken hierover zijn te vinden op Intranet. Privacy en informatiebeveiliging raken elkaar op verschillende vlakken. Eén van deze vlakken, is de bescherming van persoonsgegevens. Waar de AVG handvatten biedt over hoe om te gaan met persoonsgegevens, ziet informatiebeveiliging op de bescherming en beveiliging van alle gegevens. Zowel informatiebeveiliging als privacy vragen om een risicogedreven aanpak. Het privacybeleid en informatiebeveiligingsbeleid dragen eraan bij dat er binnen WSRL duidelijke richtlijnen zijn over hoe we omgaan met de bescherming van persoonsgegevens. Wij vinden het belangrijk dat dit op een uniforme wijze gebeurt zodat (persoons)gegevens waterschapsbreed en consequent goed beschermd worden.

Eindverantwoordelijke

Het College van dijkgraaf en heemraden (CDH) is eindverantwoordelijk voor de rechtmatige, zorgvuldige en transparante verwerking van persoonsgegevens binnen WSRL. Dit geldt ook voor de verwerkingen van persoonsgegevens die ter beschikking worden gesteld aan derden of worden gedeeld in samenwerkingsverbanden.

Het CDH stelt het beleid en de uitvoeringsmaatregelen vast op het gebied van verwerkingen van persoonsgegevens met inachtneming van de aanbevelingen van de Functionaris Gegevensbescherming. Het CDH bevordert de beschikbaarheid van voldoende middelen om uitvoering van het privacybeleid te waarborgen. Naleving van de privacywetgeving is de verantwoordelijkheid van het College van dijkgraaf en heemraden.

Portefeuillehouder privacy

Het CDH stelt een portefeuillehouder Privacy aan. Deze is gemandateerd voor het naleven van, en de controle op het beleid. De portefeuillehouder Privacy is ambassadeur voor het uitdragen van het belang van een goede organisatie van privacy en ziet erop toe dat privacy een vast onderdeel van de bedrijfsvoering wordt. Binnen WSRL is de secretaris- directeur (SD) aangewezen als portefeuillehouder Privacy.

In het kader van een rechtmatige, zorgvuldige en transparante verwerking van persoonsgegevens hanteert WSRL naast het Privacybeleid, aanvullend het Bewaartermijnenbeleid persoonsgegevens en het Beleid Personeelsvolgsystemen (PVS). Eens per drie jaar, of eerder indien nodig, worden de beleidstukken geactualiseerd.

Instemmingsrecht Ondernemingsraad

In het eerste lid van artikel 27 Wet op de ondernemingsraden (WOR) is bepaald over welke besluiten de organisatie instemming behoeft van de ondernemingsraad. Dit is onder andere het geval indien een regeling wordt vastgesteld of gewijzigd omtrent het verwerken van alsmede de bescherming van de persoonsgegevens.

3. Uitgangspunten en normen

Grondslag AVG en Wpg

Op grond van de AVG en Wpg moet de organisatie een grondslag hebben om persoonsgegevens rechtmatig te verwerken. Persoonsgegevens worden door WSRL slechts verwerkt in overeenstemming met deze wet en kunnen gebaseerd zijn op de volgende grondslagen:

1. *toestemming van de betrokkene;*
2. *noodzakelijk ter uitvoering van de overeenkomst;*
3. *wettelijke taak/verplichting;*
4. *publieke taak;*
5. *vitaal belang van de betrokkene en*
6. *gerechtvaardigd belang.*

Voor de verwerking van persoonsgegevens door opsporingsdiensten staan de grondslagen in de Wpg:

1. *ter uitvoering van de politietaak;*
2. *voor de handhaving van de openbare orde;*
3. *voor de opsporing en vervolging van strafbare feiten;*
4. *voor de uitvoering van taken op grond van de Vreemdelingenwet 2000 en*
5. *het normenkader van de Wpg is grotendeels gelijkluidend aan dat van de AVG.*

Verwerking van persoonsgegevens op strafrechtelijke grond moet voldoen aan de vereisten van de Wet politiegegevens. De opsporing van strafbare feiten door bijzondere opsporingsambtenaren (boa's) valt daarmee buiten het bereik van de AVG. Alle andere verwerkingen - waaronder het toezicht - vallen nog wel onder de AVG. WSRL heeft daarmee bij de verwerking van persoonsgegevens bij handhavingstaken te maken met zowel de AVG als de Wpg. Dit betekent dat Waterschap WSRL binnen de bedrijfsvoering rekening houdt met voorschriften en verplichtingen uit beide wettelijke regimes.

Rechtmatige verwerking

WSRL verwerkt alleen persoonsgegevens als er sprake is van één van de bovengenoemde grondslagen. Daarnaast mogen persoonsgegevens alleen verwerkt worden als daarvoor een duidelijk en gerechtvaardigd doel is vastgesteld. De gegevens die voor dit vastgestelde doel worden verwerkt worden niet voor andere doeleinden gebruikt. De doelen waarvoor WSRL persoonsgegevens verwerkt komen voort uit de wettelijke en publieke taken van WSRL in de rol van overheidsorganisatie en/of werkgever. Daarnaast moet de verwerking ten aanzien van betrokkene transparant en behoorlijk zijn.
Ook geldt dat de verwerking proportioneel en subsidiair moet zijn. Er dient een gedegen afweging plaats te vinden tussen de gebruikte gegevens en de inbreuk op privacy. WSRL hanteert het principe van dataminimalisatie. WRSL verwerkt alleen persoonsgegevens die noodzakelijk zijn voor het specifieke doel. Dit principe helpt om de privacy risico's te beperken en de rechten van betrokkenen te beschermen.

4. Werkwijze en verantwoording

Externe en interne audits

De AVG vraagt van WSRL ten aanzien van verwerkingen zich te verantwoorden en aantoonbaar te maken dat zij voldoen aan de regels op het gebied van persoonsgegevensbescherming. WSRL laat interne en externe AVG-, PDCA- en Wpg audits uitvoeren in het kader van continue verbetering. Om dit te sturen hanteert WSRL de uitgangspunten van het controle domein van de 'CIP Privacy Baseline'.

Om aantoonbaar in controle te zijn heeft WSRL CIP Privacy Baseline criteria vastgesteld. De functionaris gegevensbescherming voert periodiek controles en rapportages uit om de consistentie en juistheid van de gegevens te waarborgen. Zie Bijlage 2: CIP Privacy Baseline criteria.

In het kader van de AVG werden in 2021 en 2023 externe audits uitgevoerd. In het kader van de Wpg is eens per 4 jaar een externe audit verplicht. WSRL heeft in 2022 een eerste verplichte externe audit Wpg laten uitvoeren. Tevens is het verplicht om elk jaar een interne audit Wpg uit te voeren. Binnen WSRL wordt elk jaar, door de afdeling Concern Control, een onafhankelijke interne audit Wpg uitgevoerd.

Privacy- en gegevensbeschermingstoezicht

Binnen WSRL worden er persoonsgegevens verwerkt onder zowel extern als intern toezicht. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van privacyregels in Nederland. Daarnaast heeft WSRL een interne toezichthouder, de functionaris gegevensbescherming, die de naleving van de AVG en Wpg binnen de organisatie bewaakt. Daarnaast zijn er privacy officers aangesteld om de organisatie op het gebied van privacy te ondersteunen. De Chief Information Security Officer houdt toezicht op en adviseert over informatieveiligheid.

Register van verwerkingsactiviteiten

WSRL verwerkt weinig bijzondere persoonsgegevens. De schaalgrootte van deze verwerkingen mag, in verhouding tot andere overheden zoals bijvoorbeeld gemeenten of belastingsamenwerkingen, als beperkt worden gezien.

AVG en Wpg verplichten tot het bijhouden van een register van verwerkingen. WSRL is verantwoordelijk voor het aanleggen en bijhouden van een overzicht van alle verwerkingen waarvan WSRL de verwerkingsverantwoordelijke is in een register. Hoog risicoverwerkingen zijn ook in dit register in kaart gebracht. Hoog risicoverwerkingen zijn verwerkingen inzake de personeelsadministratie, handhaving, vergunningen, juridische zaken, contractbeheer, onderhoud, inspectie postregistratie, archivering en de inzet van personeelsvolgsytemen en AI systemen (Artificial Intelligence).

Bij WSRL vindt een continue monitoring plaats: gedurende het jaar worden tussentijdse uitkomsten van Data Protection Impact Assessments (DPIA's) en geconstateerde procesaanpassingen gebruikt om het verwerkingsregister te actualiseren. Aanvullend door middel van een jaarlijkse cyclus worden per afdelingsteam de processen besproken en geëvalueerd om het verwerkingsregister wel of niet aan te passen. Ook bij de afdeling handhaving wordt toezicht door de FG gehouden, door middel van een analyse over naleving van de rechtmatigheid van politiegegevens (Wpg). Jaarlijks wordt het geactualiseerde verwerkingsregister aan de secretaris -directeur ter akkoord aangeboden en vastgesteld. Elke verwerking in het register bevat een beschrijving van de bedrijfsactiviteit en welke gegevens daarvoor worden gebruikt. Hierdoor borgt WSRL dat de jaarlijkse toetsing van gegevensverwerkingen en de verwerkingsregister-update effectief worden uitgevoerd.

Inzet van personeelsvolgsystemen.
Bij WSRL zijn meerdere personeelsvolgsystemen (PVS) in gebruik; bijvoorbeeld voor cameratoezicht, inzet van drones, ritregistratiesystemen, smartphones, tablets en laptops, printers, OV-kaarten (NS-Businesscard), toegangspassen, vangstregistratiesysteem en bodycams.

De gegevens die worden gegenereerd uit de PVS gebruikt WSRL alleen voor het doel waarvoor de voorziening wordt ingezet. De gegevens worden niet gebruikt voor het systematisch volgen of controleren op aanwezigheid, gedrag of prestatie van medewerkers. Voor ingebruikname van PVS en wijzigingen in het gebruik geldt een instemmingsrecht van de ondernemingsraad (OR).

Voor het beleid van de diverse PVS is binnen WSRL een aanvullend Beleid personeelsvolgsystemen opgesteld. Dit beleid gaat verder in op de waarborging van de actualiteit van de PVS en het zorgvuldig omgaan met persoonsgegevens conform de AVG. Dit aanvullende beleid geeft aan wat WSRL belangrijk vindt bij het gebruik van PVS. Waarom PVS worden gebruikt en welke verantwoordelijkheden er zijn binnen de organisatie.

Beveiliging van verwerkte persoonsgegevens
WSRL is verantwoordelijk voor de bescherming van persoonsgegevens. Dit betekent dat WSRL het proces en de organisatie zo moet inrichten dat alle persoonsgegevens passend beveiligd worden. Hiervoor wordt, waar mogelijk, aangesloten bij het informatiebeveiligingsbeleid van WSRL, de Baseline Informatiebeveiliging Overheden en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

WSRL zorgt ervoor dat de persoonsgegevens die worden verwerkt zelf of door derden afdoende zijn beveiligd met technische en/of organisatorische maatregelen. Dit moet voorkomen dat persoonsgegevens onwettig kunnen worden verwerkt en dat inzage of verwerking plaatsvindt door iemand die daar geen recht toe heeft. De wijze waarop WSRL dit doet staat vermeld in het informatiebeveiligingsbeleid van WSRL. De medewerkers zijn al, mede op basis van de BIO, verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen. De geheimhoudingsplicht is voor vaste werknemers van WSRL verankerd in de ambtseed of -belofte. Tijdelijke werkkrachten die toegang hebben tot persoonsgegevens moeten een integriteits- en geheimhoudingsverklaring ondertekenen.

Privacy Risico Analyse / Data Protection Impact Assessment (DPIA)
WSRL past eerst een zogenaamde pre-scan DPIA toe. Dit is een verkorte vragenlijst om te beoordelen of een volledige DPIA noodzakelijk is. Deze is opgesteld door het CIP (Centrum informatiebeveiliging en Privacybescherming) en baseert zich daarbij op de negen criteria voor een verplichte DPIA van de European Data Protection Board en de lijst van de Autoriteit Persoonsgegevens (AP) met typen verwerkingen waarvoor een DPIA altijd verplicht is. Voor een DPIA hanteert WSRL het model van de Rijksdienst. Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy.

WSRL is voor hoog risicoverwerkingen en systemen waar gebruik gemaakt wordt van Artificial Intelligence (AI) verplicht een Data Protection Impact Assessment uit te voeren om de nodige technische- en organisatorische maatregelen te treffen volgens artikel 32 AVG.

Privacy by Design en Privacy by Default
WSRL houdt bij het ontwikkelen van nieuwe diensten, systemen of processen altijd rekening met privacy en gegevensbescherming om een optimale bescherming van persoonsgegevens te waarborgen. Dit principe staat bekend als Privacy by Design (PbD). WSRL zorgt ervoor dat concrete maatregelen zoveel mogelijk worden geïntegreerd in het ontwerp. Een voorbeeld hiervan is de aanschaf van het BOA registratie systeem dat passende technische en organisatorische maatregelen treft inzake het specifieke doel van de Wpg verwerkingen. Aanvullende werkinstructies versterken deze aanpak. Hierbij hanteert

WSRL het principe van Privacy by Default: de standaardinstellingen zijn altijd zo privacy vriendelijk als mogelijk.

Bewaartermijnen en vernietiging
In de AVG staat geen concrete bewaartermijn voor persoonsgegevens. Het uitgangspunt is dat persoonsgegevens niet langer dan noodzakelijk bewaard mogen worden. WSRL kan persoonsgegevens langer bewaren op basis van wettelijke verplichtingen zoals o.a. de Wet politiegegevens (Wpg), de Archiefwet 1995, de Waterwet, de Algemene wet bestuursrecht (Awb) of de AWR (Algemene wet inzake Rijksbelastingen). Daarnaast hanteert WSRL de Selectielijst waterschappen, een document specifiek voor waterschappen dat richtlijnen bevat voor bewaartermijnen en vernietiging van gegevens. Mocht er geen sprake zijn van een wettelijke verplichting dan bewaart WSRL de persoonsgegevens niet langer dan nodig is voor de uitvoering van de taken. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd.

Politiegegevens onder de Wpg worden ook niet langer bewaard dan strikt noodzakelijk is. Politiegegevens mogen tot maximaal vijf jaar worden bewaard. Binnen deze termijn of bij het verstrijken ervan dient definitieve vernietiging plaats te vinden, tenzij de gegevens van cultureel of historisch belang zijn. In dat geval kan van vernietiging worden afgezien en worden de bewaareisen van de Archiefwet gevolgd.

Voor het bewaren, archiveren en vernietigen van persoonsgegevens is binnen WSRL een aanvullend Bewaartermijnenbeleid Persoonsgegevens opgesteld. Deze gaat verder in op het beleid van het bewaren van persoonsgegevens volgens de AVG en Wpg, de toepassing van de verschillende wetgevingen, de momenten van gegevensverwerking, de verantwoordelijkheden, beheer en toezicht hiervan.

Informatieplicht (AVG; artikel 13 en 14)
WSRL informeert betrokkenen over welke persoonsgegevens worden verwerkt en hoe deze worden verwerkt. Op de website is dit in de privacyverklaring naar de betrokkene opgenomen. De privacyverklaring is een verkorte weergave van dit beleid. Wanneer betrokkenen gegevens aan WSRL verschaffen worden zij op de hoogte gesteld van de manier waarop WSRL de persoonsgegevens verwerkt. Indien de gegevens buiten kennisname van de betrokkene worden verkregen, worden zij, zo nodig, afzonderlijk hierover geïnformeerd. WSRL past een jaarlijkse herziening en controle van privacyverklaringen toe om naleving van dit privacybeleid en transparantie te waarborgen.

Rechten van betrokkenen (AVG: artikel 12 t/m 21)
De AVG en Wpg bepalen niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden de rechten van betrokkenen genoemd.

- recht op informatie: waarom zijn de persoonsgegevens nodig? Wat gebeurt ermee? En hoelang worden ze opgeslagen;
- recht op inzage: weten welke persoonsgegevens bekend zijn bij WSRL;
- recht op rectificatie: persoonsgegevens aanvullen, corrigeren, laten verwijderen of laten afschermen wanneer dat wordt gewenst;
- recht op beperking van de verwerking: dit houdt in dat een persoon kan verzoeken om de verwerking van zijn of haar persoonsgegevens tijdelijk stop te zetten bijvoorbeeld in het geval dat de juistheid van de gegevens wordt betwist of wanneer de verwerking onrechtmatig is;
- recht om vergeten te worden: wanneer WSRL toestemming heeft om gegevens te verwerken kunnen deze gegevens op verzoek ook weer worden verwijderd. WSRL voldoet hieraan, tenzij er gerechtvaardigde gronden zijn voor verwerking.
- recht op het overdragen van gegevens: persoonsgegevens kunnen worden opgevraagd bij de verwerkingsverantwoordelijke (bijv. WSRL) met het doel deze over te dragen aan een andere verwerkingsverantwoordelijke en
- recht op bezwaar: er kan bezwaar worden gemaakt tegen de verwerking van persoonsgegevens door WSRL.

Met deze privacy rechten krijgen betrokkenen zeggenschap over de verwerking van hun eigen persoonsgegevens. Kanttekening hierbij is, dat de rechten van betrokkenen niet absoluut zijn. Verplicht een wet tot het bewaren van persoonsgegevens? Dan mag de betrokkene niet eisen dat de gegevens eerder worden vernietigd.

<u>Indienen van verzoeken</u>

Voor de uitoefening van deze rechten van betrokkenen heeft WSRL een protocol ingericht voor de behandeling van verzoeken van betrokkenen op grond van de AVG. Jaarlijkse evaluatie van dit proces vindt binnen WSRL plaats.

Weigeringsgronden
Verzoek tot uitoefening van rechten van betrokkene kan niet in alle gevallen worden gehonoreerd. Zowel de AVG als de Wpg noemen situaties waarin het recht van betrokkene kan worden beperkt. In de AVG zijn deze opgenomen onder artikel 12. In de Wpg staan deze weigeringsgronden in artikel 27. Wanneer WSRL een verzoek niet kan honoreren, zal dit aan de betrokkene(n) worden toegelicht.

Privacy bewuste organisatie/ Awareness

Medewerkers van WSRL zijn zich bewust van de noodzaak om persoonsgegevens van medewerkers, burgers en andere betrokkenen veilig en discreet te behandelen. Medewerkers zijn en worden getraind in het beschermen van persoonsgegevens en aspecten van informatiebeveiliging. Er wordt periodiek voor nieuwe medewerkers een basistraining AVG gehouden.
Daarnaast worden voor de Privacy Ambassadeurs periodiek workshops verzorgd over specifieke privacy gerelateerde zaken.
Medewerkers worden verder geïnformeerd hoe met datalekken om te gaan en hoe deze te voorkomen. Dit gebeurt tijdens de privacy trainingen en via communicatiekanalen. Periodiek worden realistische dataleksimulaties per mail uitgevoerd om de reactievaardigheden van medewerkers te verbeteren en hun bekendheid met protocollen te vergroten. Tevens loopt er een “Waterdicht” onlinetraining met de focus op informatiebeveiliging, privacy en fysieke beveiliging voor alle medewerkers. De communicatieadviseur draagt zorg voor de uitvoering van het awareness programma privacy binnen WSRL.
Op teamniveau wordt de ontwikkeling van het deelnamepercentage gemonitord. Er is generiek trainingsmateriaal dat voor iedereen beschikbaar is gesteld.

Melden en afhandelen datalekken

Voor het melden, beoordelen en afhandelen van datalekken hanteert WSRL een datalekprotocol. Doel van dit protocol is het tijdig melden, opvolgen en sluiten van datalekken om potentiële negatieve gevolgen voor betrokkenen te voorkomen of te beperken. Dit proces voorziet in een meld- en opvolgingsproces voor privacy-incidenten en datalekken.
WSRL beziet, gelet op de omvang, ernst en risico’s, of het noodzakelijk is om dit te melden aan de Autoriteit Persoonsgegevens. De privacy officers zijn in de lead van de verdere opvolging. Privacy officers en de functionaris gegevensbescherming maken de inschatting van de ernst en kiezen in overleg de opvolging.
Indien WSRL heeft besloten dit te moeten melden, dan wordt dit uiterlijk 72 uur nadat er kennis van de inbreuk is genomen aan de AP gemeld. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. In het geval dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen, dan meldt WSRL dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd op initiatief van de functionaris gegevensbescherming.

De FG rapporteert jaarlijks aan het CDH en de secretaris directeur over het aantal meldingen, de oorzaken en de afhandeling van deze datalekken in het jaarverslag.

5. Delen van persoonsgegevens met derden

Verwerkersovereenkomst

WSRL kan een externe partij inschakelen voor het verwerken van persoonsgegevens. In geval van samenwerking met externe partijen waarbij die partij hoofdzakelijk is ingeschakeld voor het verwerken van persoonsgegevens, is die partij een verwerker. WSRL blijft verantwoordelijk voor de verwerking van de persoonsgegevens en blijft daarmee verwerkingsverantwoordelijk. Met partijen die namens WSRL persoonsgegevens verwerken wordt een verwerkersovereenkomst gesloten. Het sluiten van deze overeenkomsten is verplicht.

WSRL heeft een ‘standaardmodel Verwerkersovereenkomst met Bijlage’ ontwikkeld, die jaarlijks of zoveel eerder dan noodzakelijk wordt geactualiseerd. Dit gebeurt in samenwerking met het Waterschapshuis. Het beleid van WSRL is dat verwerkersovereenkomsten afgesloten worden conform het WSRL ‘standaardmodel Verwerkersovereenkomst met Bijlage’. In de praktijk komt het ook voor dat Verwerkers met eigen Verwerkersovereenkomsten werken. In dat geval wordt deze verwerkersovereenkomst eerst door de afdeling Juridische Zaken beoordeeld. Bij verwerkersovereenkomsten van verwerkers is de richtlijn dat de informatie uit de Bijlage van WSRL ‘standaardmodel Verwerkersovereenkomst wordt gebruikt.

Samenwerkingsverbanden
WSRL werkt samen met andere overheden en organisaties. Indien er tussen deze organisaties doorgifte en/of verwerking van persoonsgegevens plaatsvindt als onderdeel van de overeengekomen samenwerking waarbij beide organisaties allebei verwerkersverantwoordelijken zijn, worden er aanvullend op de samenwerkingsovereenkomst afspraken gemaakt over de uitwisseling van persoonsgegevens. De Belasting Samenwerking Rivierenland (BSR) en AQUON (beide zijn gemeenschappelijke regelingen waar WSRL in deelneemt) zijn voorbeelden van samenwerkingsverbanden. Deze zelfstandige rechtspersonen zijn eigenstandig verwerkingsverantwoordelijken in de zin van de AVG met betrekking tot het verwerken van persoonsgegevens.

Doorgifte van persoonsgegevens
WSRL verwerkt in principe geen persoonsgegevens buiten de Europese Economische Ruimte (hierna te noemen EER) en kiest bij het aangaan van een overeenkomst met een leverancier in principe voor een leverancier binnen de EER. Mocht dit niet lukken dan zal WSRL door middel van een Data Transfer Impact Assessment (DTIA) aantonen dat de betreffende leverancier dezelfde waarborgen zoals die gelden binnen de EER hanteert.

6. Gerelateerde zaken

Wet open overheid (Woo)
Op grond van de Wet open overheid bestaat de mogelijkheid om een verzoek om informatie in te dienen bij WSRL. Per verzoek wordt deze op de privacyaspecten bekeken.

Wet hergebruik van overheidsinformatie
De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt WSRL of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen.

Beleidsdocumenten Waterschap WSRL
Diverse interne beleidsstukken hebben een relatie met het privacybeleid of zijn hier een nadere uitwerking van. Daar waar in dit privacybeleid wordt verwezen naar een zorgvuldige omgang met persoonsgegevens of de bescherming van privacy wordt verondersteld dat het privacybeleid daaraan ten grondslag ligt. In dit verband wordt onder meer verwezen naar het Beleid Personeelsvolgsystemen, Bewaartermijnenbeleid, de Gedragscode integriteit voor medewerkers, de Gedragscode gebruik online en offline middelen, de richtlijnen voor gebruik van sociale media, de Uitvoeringsregeling integriteitsbeleid en de servicenormen van het waterschap. Tot slot wordt in dit verband verwezen naar het Informatiebeveiligingsbeleid van WSRL.

7. PDCA Cyclus

Om te borgen dat privacy en de uitvoering ervan stelselmatig wordt geëvalueerd voor verbeteringen hanteert WSRL de zogenaamde Plan Do Check Act- cyclus (PDCA-cyclus). Om het proces van Privacy planning in de organisatie goed te borgen maakt WSRL gebruik van Privacy jaarplannen die door de afdelingen tot stand komen. Privacy planning en uitvoering is “van de 1e lijn”. De afdelingshoofden nemen de privacy maatregelen op in hun afdelingsplan.
Afdelingen zijn zelf verantwoordelijk voor de start van de PDCA- cyclus en dat het proces binnen de kaders tot stand komt. De functionaris gegevensbescherming (FG) coördineert het proces, spreekt een ieder aan op zijn rol en escaleert zo nodig en heeft een toezichthoudende rol binnen de privacy cyclus De privacy officers starten de privacy werkzaamheden op, monitoren de voortgang en bewaken de kwaliteit van de werkzaamheden uit de cyclus.

Het strategisch planningsproces (cyclus) voor Privacy plannen is sinds 2023 binnen WSRL geïntroduceerd, WSRL ziet risico gestuurd denken werken en sturen als leidraad voor de prioritering.

1. Vanuit WSRL, de afdelingsdoelen en maatschappelijke ontwikkelingen worden privacy risico's/bedreigingen geïnventariseerd.
2. Voor het komende jaar worden privacy thema's besproken en risico's in kaart gebracht en geprioriteerd. WSRL ziet risico gestuurd denken werken en sturen als leidraad voor de prioritering. De geprioriteerde maatregelen worden in een privacy plan per afdeling vastgelegd en geaccordeerd.
3. Het privacy plan per afdeling is de basis voor het implementeren en beheren van privacy maatregelen:
   a. per thema wordt aangegeven in welk kwartaal de maatregel wordt uitgevoerd.
   b. per thema zijn eigenaren van eerste en tweede lijn voor de werkzaamheden vastgelegd.
4. Door te meten/monitoren en te rapporteren door de FG vindt een halfjaarlijkse evaluatie plaats met het afdelingshoofd.
5. Aan het eind van het jaar maakt de Functionaris gegevensbescherming een evaluatierapport.
   o Dit evaluatierapport is de basis voor mogelijk verbeteringen in het aankomende privacy plan voor het komend jaar.
6. De leerelementen en verbeteringen worden in de nieuwe cyclus opgenomen.

Bovenstaand strategisch planningsproces voor privacy plannen binnen WSRL bevat de vastlegging van de complete set van privacy-maatregelen, -processen en- procedures gericht op verbeteringen.

- Plan: planvorming, beleidsvorming, risicoanalyse
- Do: implementatie
- Check: monitoring, evaluatie en controle
- Act: nemen van maatregelen ter verbetering

CIP Privacy Baseline : Uitgangspunt voor Privacybeleid en implementatie van Privacy Plannen.
In de Privacy Baseline van het Centrum Informatiebeveiliging en privacybescherming (CIP) zijn de eisen van de AVG vertaald naar concrete, hanteerbare normen die duidelijk maken wat er van organisaties wordt verlangd op beleids-, uitvoerings- en control (beheers)niveau om te voldoen aan de wettelijke verplichtingen en daarmee de privacy van betrokkenen te borgen. Door het in acht nemen van de criteria van de Privacy Baseline wordt voldaan aan de specifieke doelen van privacybescherming: afscherming, corrigeerbaarheid en transparantie.

Bij het implementeren van het privacybeleid en de invoering van de Privacy plannen zijn criteria uit de Privacy Baseline van het CIP als uitgangpunt genomen.

Sinds de invoering van Privacy plannen is in 2023 een belangrijke eerste borging van planmatige en voortdurende verbetering (PDCA-cyclus) tot stand gekomen. Privacy plannen en het privacybeleid dienen verder geïntegreerd te worden in de operationele procedures en de dagelijkse praktijk. Verbetering van gedocumenteerde procedures zal leiden tot een effectievere controle en sturing van het gehele privacy proces.

Hoe komt binnen WSRL het Privacy jaarplan tot stand:

Fase 1. Inventarisatie gesprekken (november/december)
- Alle afdelingen hebben de verantwoordelijkheid om een Privacy plan voor een komend jaar te maken. Dit als een onderdeel van het jaarplan van de afdeling (business).
- Op initiatief van het afdelingshoofd (proceseigenaar), bijgestaan door teamleiders (procesmanagers), worden afspraken gemaakt met de functionaris gegevensbescherming, bijgestaan door de privacy officers.
- Tijdens deze gesprekken vindt tevens de evaluatie plaats van het lopende privacy jaarplan van de afdeling. Verbeterpunten worden opgenomen in het privacy plan van de afdeling voor het komende jaar (Lessons Learned).
- Voor het komend jaar worden mogelijke aanpassing van processen en verwerking van persoonsgegevens in kaart gebracht met de mogelijke risico's.

Fase 2. Opstellen van Privacy afdelingsplannen (december/januari)
- Op basis van de gesprekken met de afdelingen ondersteunt de Functionaris Gegevensbescherming de afdelingen met het opstellen van een Privacy jaarplan voor het komend jaar.
- Het afdelingshoofd en teamleiders accorderen het privacy plan voor hun afdeling en stellen hiervoor resources beschikbaar.

Fase 3 Vaststelling van het WSRL Privacy Jaarplan (januari/februari)
- De Functionaris Gegevensbescherming ondersteunt WSRL om alle afdelingsjaarplannen te bundelen tot één WSRL Privacy jaarplan.
- In de bundeling van deze activiteiten worden tevens actuele privacy aangelegenheden meegenomen. Hiervoor kunnen meerdere bronnen in aanmerking komen, zoals bijvoorbeeld marktontwikkelingen, kansen, bedreigingen, aanbevelingen van audits, etc.
- De functionaris gegevensbescherming communiceert de afdelingsplannen en het totale WSRL Privacy jaarplan voor het komende jaar. De afdelingshoofden en de secretaris directeur worden in kennis gesteld.

Fase 4. Uitvoering, support en monitoring (gehele jaar)
- Gedurende het lopende boekjaar worden de afgesproken privacy activiteiten conform het Privacy plan per afdeling en voor WSRL uitgevoerd.
- Er vindt een halfjaarlijkse monitoring plaats door de Functionaris Gegevensbescherming.

Bij de afdelingen BDV (Bedrijfsvoering), VTH (Vergunningen, Toezicht en Handhaving) en IDT (Informatie en Digitalisering) worden de meeste privacy werkzaamheden in het Privacy jaarplan opgenomen. Dit heeft te maken met het feit dat deze afdelingen meer risicovolle verwerkingen van persoonsgegevens heeft t.o.v. de overige afdelingen. Overige afdelingen bepalen vooraf welke privacy werkzaamheden voor het komend jaar nodig zijn, die in het Privacy Jaarplan worden opgenomen.

Verklaring van Toepasselijkheid

WSRL streeft ernaar de verwerking van persoonsgegevens volledig te beheersen en hierover op een professionele manier verantwoording af te leggen. Dit houdt in dat WSRL op de hoogte is van de genomen maatregelen omtrent de verwerking van persoonsgegevens, een planning heeft voor nog te nemen maatregelen en dit alles heeft verankerd in een PDCA-cyclus. Bij de uitvoering van de PDCA wordt aangesloten op het bestaande risicomanagement en de planning & control cyclus van de waterschappen.

In het jaarverslag van de FG is een evaluatie van het Privacy jaarplan van het voorgaande jaar opgenomen. Hierin komen de privacy werkzaamheden naar voren die WSRL heeft uitgevoerd in de naleving inzake de verwerking van persoonsgegevens. Dit in combinatie met de toepassing van de CIP Privacy Baseline geeft aan welke privacy maatregelen aantoonbaar zijn uitgevoerd om te voldoen aan de AVG. Met de CIP Privacy Baseline als basis en de evaluatie van het Privacy Jaarplan wil WSRL aantoonbaar in controle zijn.

Organisatorisch Kader

In dit privacybeleid worden de rollen en verantwoordelijkheden beschreven. Onderstaand overzicht geeft een overzicht van de privacy activiteiten op hoofdlijnen weer.

Niveau	Activiteit	Verantwoordelijke	Documentatie	Support	Monitoring / Naleving
Strategisch	Beleidsvorming	CDH Secretaris Directeur	Privacybeleid Bewaartermijnenbeleid PVS beleid	Privacy Officers 2e lijn	FG 3e lijn
Tactisch 1e lijn	Planning	Afdelingshoofden Teamleiders	Privacy jaarplan Privacy Protocollen	Privacy Officers 2e lijn	FG 3e lijn
Operationeel 1e lijn	Uitvoering	Teamleiders Privacy Ambassadeurs Gebruikers	Uitvoeren Privacy werkzaamheden Opstellen richtlijnen en maatregelen	Privacy Officers 2e lijn	FG 3e lijn

Strategische beleidsvorming: Privacybeleid/ Bewaartermijnen beleid/ PVS beleid
Op strategisch niveau vindt de beleidsvorming met betrekking tot informatiebeveiliging en privacy plaats. Het CDH is verantwoordelijk voor de vaststelling van de beleidstukken. Voor de verdere uitwerking van het beleid en de uitvoering is de secretaris-directeur gemandateerd voor de uitvoering. De FG heeft hierin een adviserende rol.

Tactische planning: Privacy jaarplan/ Privacy Protocollen
De planning van de activiteiten met betrekking tot privacy vormt het tactische niveau. Deze activiteit valt onder de verantwoordelijkheid van het hoofd van de desbetreffende afdeling. De 1e lijn wordt hierin geadviseerd door de FG.

Operationele uitvoering van Privacy plan
De uitvoering van activiteiten met betrekking tot privacy vindt plaats op operationeel niveau. Eerstverantwoordelijke voor deze activiteit is het lijnmanagement (1e lijn). Het lijnmanagement wordt daarbij ondersteund door de privacy officers (2e lijn).

‘Three Lines Model’
In de verdeling van taken rollen en verantwoordelijkheden in de privacy processen wordt bij WSRL het principe van het ‘Three Lines Model’ toegepast. Deze methodiek verdeelt risicobeheer in drie niveaus: de eerste lijn beheert risico's in het dagelijkse werk, de tweede lijn ondersteunt en monitort en de Functionaris Gegevensbescherming, de derde lijn, houdt toezicht en controleert onafhankelijk de effectiviteit van het risicobeheer. Als onderdeel van de eerste lijn worden de proceseigenaren en -managers ondersteund door de privacy officers voor de processen met verwerking van persoonsgegevens die onder zijn of haar verantwoordelijkheid vallen.

Overzicht van rollen en verantwoordelijkheden volgens het ‘Three Lines Model’
1e lijn
Het is vanuit de Privacywetgeving bepaald dat afdelingen de verantwoordelijkheid hebben om persoonsgegevens correct te verwerken en afdoende te beveiligen. Het inschatten van privacy risico’s en het handelen ernaar is een onderdeel van hun ‘core’ business.

Afdelingshoofden (proceseigenaar) 1e lijn
Afdelingshoofden hebben de tactische verantwoordelijkheid om privacy plannen te maken, te monitoren en te evalueren. Afdelingen hebben de verantwoordelijkheid om een Privacy plan voor een komend jaar te maken. Dit als een onderdeel van het jaarplan van de afdeling (business).

Teamleiders (procesmanager) 1e lijn
De operationele verantwoordelijkheid ligt bij de teamleiders. Deze zijn verantwoordelijk voor de verwerkingen en het beheer van persoonsgegevens die plaatsvinden binnen hun team op de betreffende afdeling. Teamleiders zijn medeverantwoordelijk voor het creëren van bewustwording en de naleving van het privacybeleid binnen de werkprocessen van de eigen afdeling.

Privacy Ambassadeurs 1e lijn
De teamleiders worden ondersteunt door hun privacy ambassadeurs. Een privacy ambassadeur is een medewerker van het team die de verwerking van de persoonsgegevens binnen zijn/haar team coördineert en verbeterpunten signaleert. Deze persoon is vaak het eerste aanspreekpunt voor medewerkers van

het team in de betreffende afdeling. De Privacy Ambassadeurs staan ook in direct contact met de privacy officers.

Bevoegd Functionarissen (Wpg) 1e lijn
De Wpg is bij WSRL van toepassing binnen de afdeling Vergunningen, Toezicht en Handhaving. Hier werken Buitengewoon Opsporingsambtenaren (BOA's) die persoonsgegevens verwerken. Voor de operationele uitvoerende strafrechtelijke Wpg-taken (strafbare feiten) zijn twee Bevoegd Functionarissen (BF's) aangesteld. De taken zijn over de twee personen verdeeld, met dien verstande dat zij elkaars werkzaamheden kunnen uitvoeren. De Bevoegd Functionarissen werken nauw samen met de Functionaris Gegevensbescherming en de privacy officers.

2e lijn
De privacy officers ondersteunen de organisatie bij het invullen van de verplichtingen waaraan WSRL in het kader van de AVG dient te voldoen. Zij adviseren, ondersteunen en monitoren de afdelingen/teams inzake de invulling van verplichtingen uit de AVG, zoals bijvoorbeeld de afhandeling van een melding van een (mogelijk) datalek, opstellen van een risicoanalyse (DPIA) en een verwerkersovereenkomst. Binnen WSRL zijn de privacy officers (PO's) benoemd en de resources zijn belegd binnen de afdeling Bedrijfsvoering. De verschillende taken zijn over drie personen (PO's) verdeeld, met dien verstande dat zij elkaars werkzaamheden kunnen uitvoeren.

Privacy Team 2e lijn

Het Privacy team adviseert en ondersteunt de 1e lijn in privacy kwesties en is aanspreekpunt. Het Privacy team bestaat uit de Privacy Officers en een adviserende Functionaris Gegevensbescherming.

3e lijn
De Functionaris Gegevensbescherming (FG) is de interne toezichthouder op de naleving van de AVG en Wpg binnen WSRL. De FG voert onafhankelijk toezicht, geeft advies, en rapporteert rechtstreeks aan het CDH. WSRL dient te zorgen dat de FG genoeg middelen, autoriteit en autorisaties heeft om de toezichthoudende taken te kunnen vervullen.

8. Slotbepalingen

Dit beleid treedt in werking met ingang van de eerste dag na bekendmaking in het Wetenschapsblad en wordt aangehaald als Privacybeleid Waterschap Rivierenland 2025.
[Bovenstaande zin bevat een kennelijke verschrijving. Hier wordt bedoeld: Dit beleid treedt in werking met ingang van de eerste dag na bekendmaking in het Waterschapsblad en wordt aangehaald als Privacybeleid Waterschap Rivierenland 2025.]

Het Privacybeleid Waterschap Rivierenland 2025 is op 4 februari 2025 vastgesteld in de vergadering van het College van Dijkgraaf en Heemraden van Waterschap Rivierenland. Daarmee is het Privacybeleid Waterschap Rivierenland 2022, zoals vastgesteld op d.d. 21 juni 2022 vervallen.
[Bovenstaande zin bevat een kennelijke verschrijving. Hier wordt bedoeld: Het Privacybeleid Waterschap Rivierenland 2025 is op 18 februari 2025 vastgesteld in de vergadering van het College van Dijkgraaf en Heemraden van Waterschap Rivierenland. Daarmee is het Privacybeleid Waterschap Rivierenland 2022, zoals vastgesteld op d.d. 21 juni 2022 vervallen.]

Aldus vastgesteld in de vergadering van het college van dijkgraaf en heemraden van Waterschap Rivierenland van 18 februari 2025 te Tiel.

de secretaris-directeur,
ir. Z.C. Vonk

de dijkgraaf,
drs. T.J.A.M. Cuppen MBA

Bijlage 1 Begrippen

Bij de begripsbepalingen is zoveel mogelijk uitgegaan van de definities uit de AVG en Wpg.

Algemene termen en wetgeving
Algemene verordening gegevensbescherming (AVG):
De AVG is de Europese privacywetgeving, die sinds 25 mei 2018 in de hele Europese Unie geldt. De AVG gaat over de bescherming van persoonsgegevens.

Wet Politiegegevens (Wpg):
De Wpg is een Nederlandse wet die de rechten en de plichten van de politie zelf, maar ook die van de burger regelt, voor wat betreft het verwerken van politiegegevens. De Wpg regelt de verwerking van persoonsgegevens voor de uitoefening van de politietaak door onder meer de politie en de bijzondere opsporingsdiensten (BOD), waaronder buitengewone opsporingsambtenaren (boa's) vallen.

Politiegegevens:
Politiegegevens als bedoeld in de Wet politiegegevens (Wpg). In dit beleid worden met persoonsgegevens ook politiegegevens bedoeld, tenzij dit anders is bepaald.

Persoonsgegevens:
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat ofwel indirect naar deze persoon te herleiden is.

Bijzondere persoonsgegevens:
Dit zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

Verwerking van persoonsgegevens:
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens zoals bijvoorbeeld het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerkingen:
De verwerking van persoonsgegevens of politiegegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen.

Verwerkingsverantwoordelijke:
Een persoon of instantie die alleen of samen met een ander het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerker:
De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van de verwerkersverantwoordelijke.

Betrokkene:
De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

Rollen en verantwoordelijkheden
Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens (AP) is de onafhankelijke toezichthouder op de naleving van de privacywetgeving in Nederland. De AP handhaaft de regels uit de Algemene Verordening Gegevensbescherming (AVG) en andere privacygerelateerde wetten, behandelt klachten van betrokkenen en geeft voorlichting over de bescherming van persoonsgegevens.

Functionaris voor de gegevensbescherming (FG):
De Functionaris Gegevensbescherming (FG) is de interne toezichthouder op de naleving van de AVG en Wpg binnen WSRL. De FG voert onafhankelijk toezicht, geeft advies, en rapporteert rechtstreeks aan het CDH. WSRL dient te zorgen dat de FG genoeg middelen, autoriteit en autorisaties heeft om de toezichthoudende taken te kunnen vervullen. Vanwege zijn onafhankelijke rol is de functie van FG binnen WSRL belegd bij het Team Concerncontrol.

Chief Information Officer (CIO):
De Chief Information Officer (CIO) is verantwoordelijk voor de strategische aansturing van informatievoorziening binnen een organisatie. De CIO waarborgt dat IT-investeringen bijdragen aan de strategische doelen van de organisatie en dat informatieveiligheid en privacy goed zijn verankerd in het beleid.

Chief information security officer (CISO):
De Chief Information Security Officer (CISO) is verantwoordelijk voor het strategisch beleid rondom informatieveiligheid binnen de organisatie. De CISO bewaakt en stuurt de ontwikkeling, implementatie en naleving van informatiebeveiligingsbeleid, waarbij hij/zij de integriteit, beschikbaarheid en vertrouwelijkheid van informatie borgt. De CISO speelt een adviserende rol in het privacybeleid door ervoor te zorgen dat technische en organisatorische maatregelen voldoen aan wet- en regelgeving zoals de AVG en de BIO (Baseline Informatiebeveiliging Overheid). De CISO werkt nauw samen met de Functionaris Gegevensbescherming (FG) om te zorgen voor een integrale aanpak van privacy en informatieveiligheid.

Information security officer (ISO):
De Information Security Officer (ISO) is verantwoordelijk voor de operationele implementatie van het informatiebeveiligingsbeleid binnen de organisatie. De ISO ondersteunt afdelingen bij het toepassen van beveiligingsmaatregelen en bewaakt de dagelijkse naleving van richtlijnen en protocollen. In relatie tot het privacybeleid draagt de ISO zorg voor het technisch beveiligen van persoonsgegevens, zoals het toepassen van encryptie, toegangsbeheer en logging. De ISO werkt in de eerste lijn en rapporteert bevindingen en risico's aan de CISO, zodat strategische maatregelen kunnen worden genomen. De ISO vormt een belangrijke schakel in het voorkomen van datalekken en de bescherming van persoonsgegevens

Privacy officer (PO):
Privacy Officers zijn tactische en operationele specialisten die binnen de organisatie ondersteunen bij de naleving van privacywet- en regelgeving, zoals de AVG en Wpg. Ze adviseren afdelingen over privacyvraagstukken, ondersteunen bij het uitvoeren van privacy-analyses (zoals DPIA's), en coördineren activiteiten zoals het opstellen en actueel houden van verwerkersovereenkomsten en het register van verwerkingsactiviteiten. Privacy Officers zijn een verbindende schakel tussen de Functionaris Gegevensbescherming (FG) en de operationele teams en spelen een cruciale rol in het bevorderen van privacybewustzijn binnen de organisatie. Daarnaast monitoren ze de naleving van het privacybeleid, ondersteunen bij het melden van datalekken, en signaleren verbeterpunten voor processen waarin persoonsgegevens worden verwerkt.

Privacy Ambassadeurs (PA):
Een privacy ambassadeur is een medewerker van het team die de verwerking van de persoonsgegevens binnen zijn/haar team coördineert en verbeterpunten signaleert. Deze persoon is vaak het eerste aanspreekpunt voor medewerkers van het team in de betreffende afdeling. De Privacy Ambassadeurs staan ook in direct contact met de privacy officers.

Bevoegd Functionaris (BF):
De BF ondersteunt de organisatie bij de toepassing, uitvoering en de naleving van de Wet Politiegegevens (Wpg) in de dagelijkse werkzaamheden.

Procesmanager
De procesverantwoordelijke is degene die eigenaar is van het bedrijfsproces waarbinnen de applicatie wordt gebruikt. Deze persoon bewaakt de effectiviteit en efficiëntie van het proces en zorgt ervoor dat het proces en het gebruik van de applicatie op elkaar afgestemd zijn. Dit is meestal de teamleider en rapporteert aan de proceseigenaar.

Proceseigenaar / Applicatie eigenaar:
Deze persoon is verantwoordelijk voor het proces/ de applicatie als geheel, inclusief de juridische en beleidsmatige kant. Hij of zij zorgt ervoor dat het gebruik van de technologie voldoet aan de wettelijke vereisten. Dit is meestal het afdelingshoofd. Rapporteert aan de verantwoordelijke directeur.

Functioneel beheerder:
Deze rol richt zich op de dagelijkse operationele aansturing en toepassing van de applicatie. De functioneel beheerder schrijft werkinstructies, houdt toezicht op het correcte gebruik en borgt dat het proces voldoet aan de geldende richtlijnen en instructies. Hij is vaak degene die rechtstreeks communiceert met gebruikers en zorg draagt voor naleving van het proces.

Applicatiebeheerder of technisch beheerder:

Dit is de technisch specialist die zich vooral bezighoudt met de technische werking en het onderhoud van de applicatie. De technisch beheerder werkt samen met de functioneel beheerder en de proceseigenaar om te zorgen voor de technische uitvoering.

De Gebruiker:
Is verantwoordelijk voor het naleven van het beleid omtrent gegevensbewaring en heeft de plicht om persoonsgegevens en andere vertrouwelijke informatie binnen de gestelde bewaartermijnen correct te beheren. Dit betreft medewerkers en externen betrokkenen.

Processen

CIP Privacy Baseline:
De Privacy Baseline is een document voor professionals die hands-on in de organisatie werken aan privacy maatregelen en de borging van en de controle op die maatregelen. Het is een naslagwerk waarin de eisen van de AVG vertaald zijn naar concrete, hanteerbare normen.

'Three Lines Model'
Deze methodiek verdeelt risicobeheer in drie niveaus: de eerste lijn beheert risico's in het dagelijkse werk, de tweede lijn ondersteunt en monitort en de Functionaris Gegevensbescherming, de derde lijn, houdt toezicht en controleert onafhankelijk de effectiviteit van het risicobeheer. Als onderdeel van de eerste lijn worden de proceseigenaren ondersteund door de Privacy Officers voor de processen met verwerking van persoonsgegevens die onder zijn of haar verantwoordelijkheid vallen.

Privacy By Design en Default (PbDD):
Bij Privacy By Design wordt in zo vroeg mogelijk stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens afgedwongen. Privacy By Default vereist dat de standaardinstellingen altijd zo privacy vriendelijk mogelijk zijn.

Data Protection Impact Assessment (DPIA):
Met een DPIA worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van privacy.

Data Transfer Impact Assessment (DTIA):
Een DTIA is een risicobeoordeling voor de doorgifte van persoonsgegevens naar derde landen.

PVS (Personeelsvolgsysteem):
Een personeelsvolgsysteem is het technische en organisatorische samenspel, dat wil zeggen het geheel van apparatuur, programmatuur en bijbehorende administratieve organisatie, dat het mogelijk maakt om het gedrag en de prestaties van medewerkers tijdens en buiten het arbeidsproces te registreren. Hier kunnen al dan niet bewust conclusies aan worden verbonden.

Overige definities
AI-systemen:
Kunstmatige intelligentie (KI) of artificiële intelligentie (AI) is het nabootsen van menselijke vaardigheden met een computersysteem, zoals: het aanleren, redeneren, anticiperen en plannen om zichzelf automatisch bij te sturen. Het kan zelfstandig beslissen, zonder tussenkomst van menselijke intelligentie.

Waterschapshuis:
Het Waterschapshuis is er voor alle 21 waterschappen in Nederland. Zij hebben gezamenlijk de Gemeenschappelijke Regeling het Waterschapshuis ingesteld om overkoepelend samen kennis te delen en te werken aan programma's en projecten. In dit beleid gericht op AVG en Wpg.

Bijlage 2. CIP Privacy Baseline criteria

In de Privacy Baseline van het Centrum Informatiebeveiliging en privacybescherming (CIP) zijn de eisen van de AVG vertaald naar concrete, hanteerbare normen die duidelijk maken wat er van organisaties wordt verlangd op beleids-, uitvoerings- en control (beheers)niveau om te voldoen aan de wettelijke verplichtingen en daarmee de privacy van burgers te borgen. Door het in acht nemen van de criteria van de Privacy Baseline wordt voldaan aan de specifieke doelen van privacybescherming: afscherming, corrigeerbaarheid en transparantie. Bij het implementeren van het privacybeleid zijn criteria uit de Privacy Baseline van het CIP bij WSRL als uitgangpunt genomen.

De 'Privacy Baseline is verdeeld in de volgende drie hoofdstukken:
1. Het Privacybeleid van organisaties (Beleidsdomein);
2. De eisen aan de uitvoering van de AVG (Uitvoeringsdomein), en:
3. 3. Het beheer en de controle van het privacybeleid (Control- of Beheerdomein).

De CIP Baseline criteria (KPI's) zijn de uitgangspunten voor de invoering Privacy Plannen. Onderstaande KPI's worden binnen WSRL gebruikt om Privacy aan te sturen. De FG rapporteert de uitgevoerde Privacy werkzaamheden in het FG jaarverslag.

Overzicht Key Performance Indicators (KPI's).

1.Beleidsdomein Werkzaamheden

Per 3 jaar Update Privacybeleid en bij extreme veranderingen incidenteel per jaar
Per 3 jaar Update Beleid Bewaartermijnen en incidenteel per jaar
Per 3 jaar Update Beleid PVS systemen en incidenteel per jaar

Organieke inbedding
Jaarlijks Inventarisatie Privacy plan WSRL komend jaar. Afdelingsgesprekken
Jaarlijks Budget bespreking Privacy Officers
Jaarlijks Afronding met afdelingen MT, vaststelling WSRL Privacy plan komend jaar.

Communicatie
Jaarlijks Minimaal 3x Trainingen / Workshops AVG voor Ambassadeurs
Jaarlijks Minimaal 3x AVG Basistraining voor nieuwe medewerkers
Jaarlijks 1x Jaarlijkse Awareness Activiteit Privacy (28 mei)
Jaarlijks Per kwartaal minimaal 3 Privacy Artikelen op STROOM plaatsen (KPI 12)

Risico management, Privacy by Design en DPIA

Jaarlijks Minimaal 2 x DPIA's per jaar uitvoeren van applicaties behorend onder Personeel Volgsystemen (Template DPIA van de Rijksoverheid)
Jaarlijks Minimaal 2 x Pre Scan DPIA's identificeren en uitvoeren
Jaarlijks Minimaal 2 x DPIA's identificeren hoog risco verwerkingen en uitvoeren.

2.Uitvoeringsdomein Werkzaamheden

Doelbinding gegevensverwerking en Register van verwerkingsactiviteiten

Jaarlijks Vaststelling van Verwerkingsregister en aan directie ter akkoord
Halfjaarlijks Toezicht door de FG: Analyse over naleving rechtmatigheid van politiegegevens (Wpg)
Continue Aanpassing van Verwerkingsregister.
Op basis van uitkomsten van DPIA's en proces aanpassingen

Kwaliteitsmanagement
Wekelijks Wekelijks overleg met Privacy Officers
Per kwartaal Bewijsvoering . Vastleggen alle bewijzen per kwartaal
Continue Identificeren nieuwe Privacy ontwikkelingen en trends voorbeelden AI, SOC, etc

Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens
Jaarlijks Jaarlijkse evaluatie en controle van Privacy verklaringen
Per drie jaar Protocol voor de behandeling van verzoeken van betrokkenen op grond van de AVG

Personeel volgsystemen

Per jaar Update van de Personeel volgsystemen (protocol)

Doorgifte persoonsgegevens

Jaarlijks Update risico gebaseerde beoordeling van verwerkers in verwerkingsregister (High Risk Check)
Jaarlijks Update Verwerkersovereenkomsten: Continue activiteit met de focus op hoog risico verwerkingen
Jaarlijks Continue update van model verwerkersovereenkomst conform Waterschapshuis

3.Control/
Beheerdomein Werkzaamheden

Intern toezicht
Jaarlijks Opstellen FG -Jaarverslag

Meldplicht Datalekken
Dagelijks Melding van Datalekken afhandelen en rapporteren
Per 6 maanden Evaluatie Datalekken en werkproces Datalek protocol
Per 6 maanden Twee realistische datalek-simulaties worden per jaar uitgezet om medewerkers te trainen. (i.s.m. Afdeling A-IDT)
Per jaar Jaarrapport FG Datalekken

Externe Audit
Per 2 jaar Externe AVG Audit in 2021,2023 en 2025
Per 4 jaar (2021 + 2025) Externe Wpg Audit (2021,2025,2029)

Interne Controle
Halfjaarlijks Halfjaarlijkse controle van de Privacy plannen per afdeling
Jaarlijks Evaluatie van de Privacy Jaarplannen voorgaand jaar
Jaarlijks Jaarlijkse interne Wpg, Hercontrole van externe Audit (2023,2024,2026)