provincie Zuid-Holland

# Privacybeleid 2024 - 2026

Versie 1.0

## Inhoudsopgave

# 1 Inleiding

Als provincie Zuid-Holland werken we met (persoons)gegevens van burgers, leveranciers, ondernemers, bestuurders en medewerkers en andere natuurlijke personen. We verzamelen gegevens om onze provinciale wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken zoals maatschappelijke vraagstukken over bereikbaarheid, energie, economie, natuur en gebiedsontwikkeling. We verwerken ook gegevens van personeel en voor interne bedrijfsvoering. We kunnen deze taken alleen goed doen, als we persoonsgegevens verwerken. Om een professionele en betrouwbare overheid te zijn, moeten we deze gegevens op een zorgvuldige en veilige manier verwerken. Betrokkenen moeten erop kunnen vertrouwen dat hun gegevens bij ons in goede handen zijn.

Ook nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitalere overheid maken het complexer en noodzakelijker om zorgvuldig om te gaan met persoonsgegevens. Wij zijn ons hiervan bewust en geven daarom met dit beleid aan hoe wij in algemene zin invulling geven aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna: AVG).

*Geldigheidsduur*

Gedeputeerde Staten (GS) zijn eindverantwoordelijke voor de provinciale gegevensverwerking en zij hebben dit beleid vastgesteld op xx-xx-2024. We beoordelen het beleid tenminste eens per vier jaar en zo nodig herzien we het. GS kunnen besluiten tot een tussentijdse herziening als:

- wetgeving of maatschappelijke urgentie leidt tot een wijziging in de principes in hoofdstuk 8 van dit beleid;
- Organisatorische veranderingen gevolgen hebben voor de beschreven verantwoordelijkheden in hoofdstuk 7 van dit beleid.

# 2 Juridisch kader

We baseren dit privacybeleid op de uitgangspunten van de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAG).

De AVG biedt binnen Europa en dus ook binnen Nederland en de provincie het wettelijk kader om persoonsgegevens te verwerken. Daarbij staat bescherming van de persoonlijke levenssfeer van betrokkenen voorop. In de Nederlandse UAVG staan regels voor uitvoering van de AVG. Er staat ook nadere wetgeving in op vlakken waar de AVG ruimte laat voor eigen invulling van de lidstaten.

Op basis van de nu geldende wetgeving, de in ontwikkeling zijnde Europese wetgeving en dit beleid kan de eenheid Privacy protocollen, instructies, processen of modellen uitgeven. De eenheid Privacy zorgt ervoor dat de actuele versies op Binnenplein, ons intranet, te vinden zijn. Dit uiteraard na vaststelling door het bevoegd gezag.

Naast de AVG en de UAVG hebben we te maken met specifieke wetgeving voor de verwerking van persoonsgegevens om strafbare feiten te voorkomen, op te sporen of te vervolgen. Als buitengewoon opsporingsambtenaren (boa's) van de provincie persoonsgegevens verwerken bij strafrechtelijke

handhaving dan valt dit niet onder de AVG maar onder de Wet politiegegevens (Wpg). De provincie heeft daarom een Privacybeleid Wpg vastgesteld.

## 3 Begripsbepalingen

Wij hanteren in dit beleidsdocument dezelfde definities als art. 4 van de AVG.

Het Centrum Informatiebeveiliging en Privacybescherming (CIP) is een publiek-private netwerkorganisatie. De eenheid Privacy hanteert de Privacy Baseline van het CIP. De Privacy Baseline vertaalt de eisen van de AVG naar concrete, hanteerbare normen die duidelijk maken wat organisaties moeten doen om de privacy van de betrokkenen te waarborgen.

## 4 Doel

Met dit privacybeleid geven wij iedereen die bij of voor de Provincie werkt het kader om verantwoord om te gaan met persoonsgegevens en waarborgen wij de persoonlijke levenssfeer van de personen waarvan wij persoonsgegevens (laten) verwerken. Daarnaast bakenen wij met dit privacybeleid taken en verantwoordelijkheden om persoonsgegevens te beschermen helder af.

De verdere uitwerking van dit beleid hebben we - waar nodig - vastgelegd in protocollen, procesbeschrijvingen, modellen en formulieren. Deze documenten zijn te vinden op de Privacy-AVG pagina op het Binnenplein.

GS hebben naast dit privacybeleid ook een informatiebeveiligingsbeleid vastgesteld. Daar staan maatregelen in om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde om persoonsgegevens te beschermen. We kunnen het provinciale privacybeleid daarom niet los zien van het provinciale informatiebeveiligingsbeleid.

## 5 Reikwijdte

Wij verzamelen en gebruiken persoonsgegevens van burgers, leveranciers, ondernemers, bestuurders en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de provincie, waaronder:

1. De verwerking van persoonsgegevens binnen onze opgaven;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd met een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan;
3. De verwerking van persoonsgegevens van personeel en interne bedrijfsvoering.

# 6 Missie, visie en doelstelling

## 6.1 Missie

Wij willen als provincie een betrouwbare overheidspartner zijn die zorgvuldig omgaat met persoonsgegevens en deze gegevens goed beschermt.

## 6.2 Visie

Een goede privacy administratie is belangrijk om onze provincie goed te laten functioneren en vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn van de hele organisatie. Ieder organisatieonderdeel en alle professionele teams moeten hierbij dus betrokken zijn. Dit is immers de basis om rechten van burgers, bedrijven, partners en andere betrokkenen te beschermen. Verantwoord en bewust gedrag van alle medewerkers is dus essentieel om privacy binnen onze provincie te waarborgen.

Om de betrouwbaarheid te meten en daarmee de mate van privacy volwassenheid te kunnen bepalen is het ‘Privacy volwassenheidsmodel’ van het CIP gebruikt. Dit model geeft aan hoe volwassen de organisatie is in borging van privacy. Het model kent vijf volwassenheidsniveaus, 1 t/m 5. Bij het laagste volwassenheidsniveau maakt een organisatie zich niet druk om privacy, bij volwassenheidsniveau 5 zijn alles aspecten geoptimaliseerd op alle niveaus binnen een organisatie. De provincie streeft ernaar om eind 2025 een volwassenheidsniveau van 3 te hebben.

## 6.3 Doelstelling

Om het gewenste volwassenheidsniveau te bereiken zal een aantal stappen doorlopen moeten worden. De eenheid Privacy is in 2022 opgericht om de organisatie te ondersteunen en te begeleiden om het gewenste privacyvolwassenheidsniveau te behalen en heeft hierin al enkele stappen gezet. Het is nu belangrijk dat op basis van dit beleid, onderliggende processen worden beschreven en vastgesteld, er meer bewustwording komt en er samen gewerkt wordt aan het zorgvuldig omgaan met persoonsgegevens.

De uitwerking van dit beleid, nodig om het gewenste volwassenheidsniveau te bereiken, is een ontwikkelopgave voor de provincie. Door een stuurgroep binnen het domein Bedrijfsvoering is een plan van aanpak opgesteld waarin de huidige privacyrisico’s met de meest aanzienlijke, directe impact zijn geanalyseerd. Dit plan van aanpak beschrijft ook de daarop volgende beheersende maatregelen die bij zullen dragen aan het stelselmatig oplossen of minimaliseren van deze privacyrisico’s. De initiële uitvoering van het plan van aanpak richt zich op de periode 2024 tot 2026. Maar de uitvoering van veel van de structurele veranderingen en beheersende maatregelen zoals beschreven in het plan van aanpak zal ook na 2026 continueren.

De eenheid Privacy draag actief hieraan bij door:

- Het verhogen van privacy bewustwording: privacy maakt onderdeel uit van de provincie-brede campagne ‘Zo doen we dat!’. Deze campagne is gericht op bewustwording en gedragsverandering zodat we nog beter kunnen omgaan met onze data. Daarnaast zal de eenheid Privacy zelf meer bewustwording creëren voor het onderwerp omgaan met persoonsgegevens door het aanbieden van AVG trainingen via de PZH-Akademie en het

deelnemen aan het onboardingprogramma voor nieuwe medewerkers. Samen met informatieveiligheid wordt ingezet op regelmatig en ook verplichte e-learnings voor alle medewerkers. Er zal ook actiever communicatie plaatsvinden op Binnenplein en er zullen diverse acties door het jaar heen worden georganiseerd.

- Verdere professionalisering van en intensieve samenwerking met de organisatie om op een zorgvuldige en verantwoorde manier persoonsgegevens te verwerken. Dit betekent dat de eenheid actief de opgaven opzoekt om deze opgaven te adviseren en te begeleiden in het werken conform het privacybeleid en de benodigde acties die volgen uit het plan van aanpak. Door aan de voorkant betrokken te zijn kan in een vroeg stadium meegenomen worden hoe invulling kan worden gegeven aan de privacywetgeving en kan samen met de opgaven meegedacht worden om het werken met persoonsgegevens binnen de kaders mogelijk te maken.

- Het structurele karakter van de rol van de eenheid Privacy: privacy moet worden gezien als regulier werk. Compliance van privacy is nooit ‘klaar’. Ook nadat volwassenheidsniveau drie is behaald, moeten we aandacht blijven besteden aan het behouden en borgen van dit niveau en verbeteringen daar waar nodig doorvoeren. Het doorlopend waarborgen van naleving aan de AVG is nodig om compliance aan de AVG en eventuele nieuwe wetgeving om persoonsgegevens te beschermen aan te tonen en om een betrouwbare overheid te creëren en te houden. De eenheid Privacy blijft de opgaven ondersteunen bij het naleven en borgen van privacywetgeving binnen de opgaven.

# 7 Verantwoordelijkheden

## 7.1 Het college van Gedeputeerde Staten

Het college van Gedeputeerde Staten (GS) is bestuurlijk eindverantwoordelijk voor het naleven van de privacy wet-en regelgeving en de kaders voor het verantwoord omgaan met persoonsgegevens. Over de uitvoering van het privacybeleid legt GS verantwoording af aan Provinciale Staten. Als verantwoordelijk gezag stelt GS het privacybeleid vast.

## 7.2 Directieteam

Het Directieteam (DT) bestaat uit de provinciesecretaris en de concerndirecteur en is ambtelijk eindverantwoordelijk voor de bedrijfsvoering van provincie Zuid-Holland en daarmee voor de uitvoering en sturing op de beleidskaders van privacy (waarbij wordt gestuurd op concernrisico's). Op basis van het privacybeleid wijst het DT taken, verantwoordelijkheden en bevoegdheden toe. Het DT heeft op basis van zijn actieve informatieplicht de verantwoordelijkheid om GS indien nodig te informeren over kritieke risico's en non-compliances op gebied van privacy.

## 7.3 Bedrijfsvoering en Concerncontrol

De domeindirecteur Bedrijfsvoering en de Concerncontroller vormen (samen met het Opgave Domein Beraad en het P-beraad) het aanspreekpunt voor GS en het DT op het onderwerp privacy binnen de opgaven en opdrachten en sturen op het borgen van de integraliteit en samenhang tussen opgaven en opdrachten. Ook zijn zij verantwoordelijk voor de inrichting van de beheersing en de sturing van de opgaven. Dit betekent dat er ook gestuurd wordt op het voldoen aan de verplichtingen uit de privacy wet- en regelgeving en het uitvoeren van het privacybeleid. De domeindirecteur Bedrijfsvoering, waar de opgave privacy onderdeel van uitmaakt, dient als escalatie voor de eenheid Privacy als er binnen de opgaven en opdrachten privacyrisico's zijn gesignaleerd die onvoldoende worden opgepakt door AOG's of domeindirecteuren. De Concerncontroller dient als uiterste escalatie voor de eenheid Privacy binnen het P-domein als privacyrisico's onvoldoende worden opgepakt door P-managers of de directeuren Mens&Organisatie.

## 7.4 Ambtelijk Opdrachtgevers en P-managers

De dagelijkse verantwoordelijkheid voor het voldoen aan de uitgangspunten van de privacy wet- en regelgeving binnen de provincie is belegd bij de Ambtelijk Opdrachtgevers (AOG's) en de P-managers. De AOG's en P-managers zorgen ervoor dat binnen de opgaven gewerkt wordt conform dit privacybeleid. De AOG geeft de Ambtelijk opdrachtnemer (AON) aanwijzingen hoe deze randvoorwaarden het beste kan invullen binnen zijn opdracht. De AOG's en P-managers zijn ervoor verantwoordelijk om binnen hun werkzaamheden de juiste disciplines, voor privacy de eenheid Privacy, hier op het juiste moment te betrekken.

## 7.5 Eenheid Privacy

De eenheid Privacy draagt actief bij aan de uitvoering van dit privacybeleid door de organisatie (medewerkers, AON's, AOG's, P-managers, directeuren M&O, domeinen, DT en GS) en het in control zijn op gebied van privacy. Onderdeel van de taak van de eenheid Privacy is het ondersteunen en

begeleiden van de organisatie bij het verhogen van het privacyvolwassenheidsniveau naar het gewenste niveau 3 in 2025.

De eenheid volgt daarbij een beleidsvormende (strategische) cyclus en een uitvoerende (operationele) cyclus. Op het snijvlak van beide cycli ligt het uitvoeringsprogramma. Vanuit een strategisch kader wordt de vertaling gemaakt naar operationeel beleid ten behoeve van kwaliteitsborging samen met een sluitende planning- en controlcyclus.

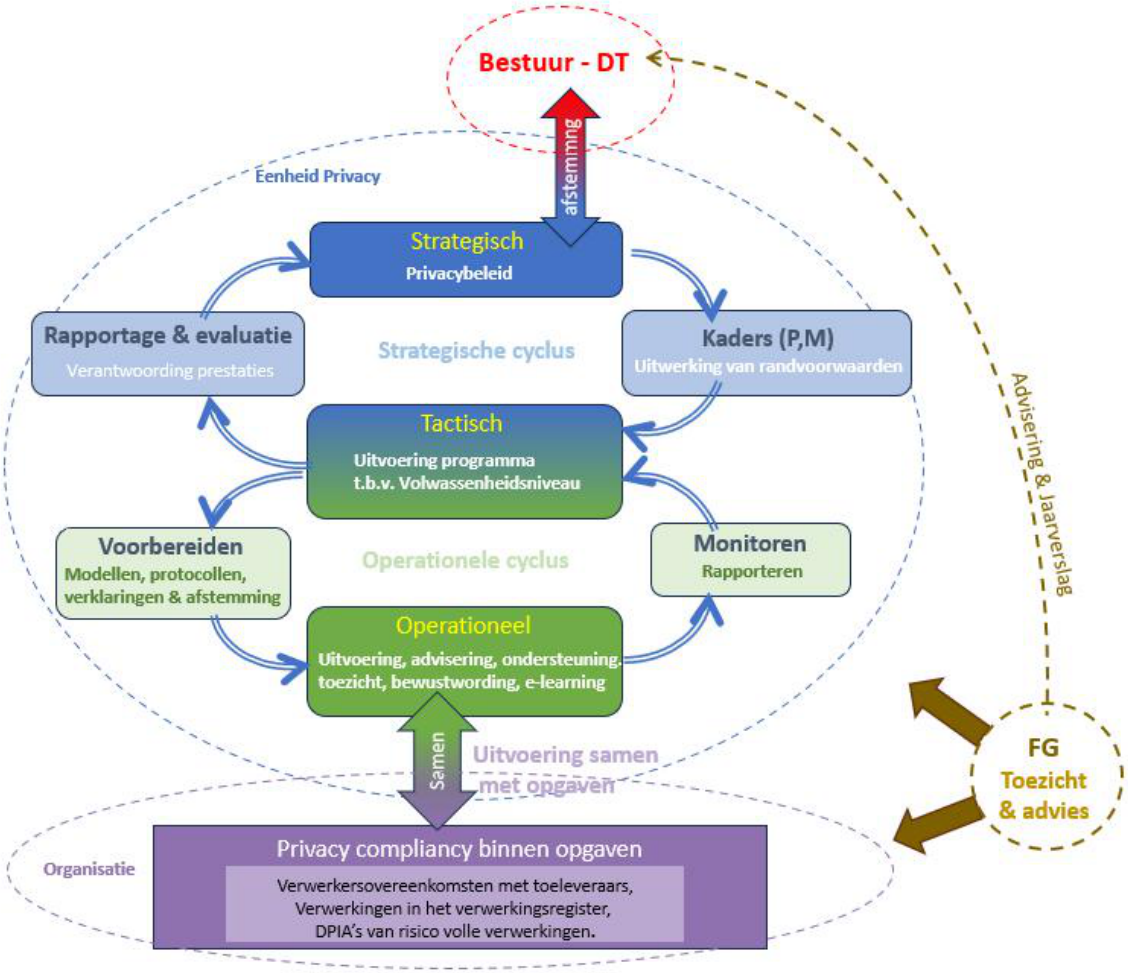
De beleidsvormende cyclus ziet op de samenwerking van de eenheid Privacy met het bestuur (GS-DT) van de provincie om beleid te maken en kaders te stellen voor het uitvoeringsprogramma. De eenheid Privacy monitort de uitvoering en evalueert en rapporteert hierover aan het bestuur. Op basis van de evaluaties en rapportages kunnen door het bestuur de benodigde aanpassingen of acties ondernomen worden in samenwerking met de eenheid Privacy.

De uitvoerende cyclus ziet op de samenwerking van de eenheid Privacy met de organisatie (domeindirecteur Bedrijfsvoering, Concerncontroller, directeuren M&O, P-managers, domein directeuren, AOG's, AON's, medewerkers) om het beleid goed uit te voeren en bestaat uit het vertalen van het uitvoeringsprogramma naar de organisatie. Dit doet de eenheid Privacy door het ontwikkelen van werkwijzen, waaronder modellen, protocollen, formulieren, etc. om de organisatie te ondersteunen bij privacy activiteiten. De eenheid Privacy heeft een belangrijke aanjagersrol in de uitvoering van het privacybeleid samen met de organisatie. Dit betekent dat de eenheid actief de opgaven opzoekt om deze opgaven te adviseren en te begeleiden in het werken conform het privacybeleid. De eenheid Privacy zorgt voor bewustwording binnen alle lagen in de organisatie en het samen met de opgaven uitvoeren van de benodigde werkzaamheden.

Als er binnen de opgaven privacyrisico's zijn gesignaleerd die onvoldoende worden opgepakt, kan de eenheid Privacy escaleren aan de AOG of domeindirecteur (O-domein). Als de privacyrisico's blijven bestaan kan de eenheid Privacy escaleren aan de domeindirecteur Bedrijfsvoering (O-domein). Binnen het P-domein escaleert de eenheid Privacy aan de directeuren Mens&Organisatie of in het uiterste geval aan de concerncontroller. Escalatie door de eenheid Privacy ziet op inhoudelijke aspecten van het omgaan met persoonsgegevens en niet op gedrag van medewerkers.

Op die manier kan de eenheid Privacy ook goed monitoren hoe de uitvoering van het beleid in de praktijk gaat en kan dit meegenomen worden in de evaluatie en rapportage aan het bestuur.

In onderstaande figuur is een uitwerking van de hierboven beschreven cycli.




## 7.6 Functionaris voor Gegevensbescherming (FG)

De provincie is op grond van de AVG en de Wpg verplicht om een FG aan te stellen. De FG heeft een onafhankelijke adviserende en toezichthoudende positie binnen de organisatie.

De organisatie is verantwoordelijk voor het opstellen en uitvoeren van het privacybeleid. De FG ziet toe op de naleving hiervan en brengt advies uit over de risico's van bestaande verwerkingen en voorgenomen nieuwe producten en diensten. Als interne toezichthouder controleert de FG of de organisatie de AVG goed toepast en ziet erop toe dat betrokkenen hun privacyrechten kunnen uitoefenen. De FG brengt jaarlijks een verslag uit aan Provinciale Staten en Gedeputeerde Staten van zijn werkzaamheden, bevindingen en aanbevelingen. Problemen met compliance bespreekt de FG direct met het bestuur van de provincie.

De FG heeft regelmatig overleg met de Chief Information Security Officer (CISO). De CISO houdt onder meer toezicht op de technische en organisatorische maatregelen binnen de organisatie om een op het risico afgestemd informatiebeveiligingsniveau te waarborgen. Deze technische en

organisatorische maatregelen zijn een voorwaarde voor privacy waardoor onderling overleg over de stand van zaken binnen de organisatie nodig is.

De uitvoerige taken van de FG zijn vastgelegd in het “Reglement functionaris voor gegevensbescherming Zuid-Holland 2018” dat is gepubliceerd in het Provinciaal blad nr. 3834 van 25 mei 2018.

Iedereen die bij of voor de provincie Zuid-Holland werkt is verantwoordelijk om zorgvuldig om te gaan met persoonsgegevens. Als provincie verlangen wij dan ook dat al onze medewerkers en alle personen die voor ons werken de kaders van dit privacybeleid opvolgen en actief uitdragen. Dit beleid en de onderliggende protocollen, processen en bewustwording ondersteunen hierbij.

# 8 Principes om persoonsgegevens te verwerken

De AVG baseert zich op een aantal principes om persoonsgegevens te verwerken. Wij onderschrijven deze principes en hebben als doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

## 8.1 Rechtmatige grondslag

Als provincie verwerken wij persoonsgegevens alleen in overeenstemming met wetgeving die op ons van toepassing is en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden als hiervoor een rechtmatige verwerkingsgrondslag bestaat. De grondslag voor een verwerking bij een provincie vloeit vaak voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak. Als de verwerking gebaseerd is op toestemming dan moeten wij kunnen aantonen dat de toestemming vrijelijk, specifiek, geïnformeerd en ondubbelzinnig is gegeven. Dit kan bijvoorbeeld via een schriftelijke verklaring, of via elektronische middelen. De eenheid Privacy stelt model toestemmingsformulieren op.

## 8.2 Welbepaalde doeleinden

Wij verwerken persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen wij geen persoonsgegevens verwerken. Wij mogen persoonsgegevens alleen verwerken als dit noodzakelijk is om het doel te bereiken waarvoor wij de gegevens ontvingen. Het doel waarvoor wij persoonsgegevens verwerken moet uitdrukkelijk zijn omschreven. Kunnen wij het doel op een andere – minder ingrijpende – wijze bereiken, bijvoorbeeld door minder of geen persoonsgegevens te verwerken, dan kiezen wij daarvoor.

## 8.3 Verdere verwerking

Persoonsgegevens verwerken voor een ander doel dan waarvoor ze in eerste instantie zijn verzameld mag alleen als er sprake is van een verenigbaar doel, specifieke toestemming van betrokkenen of op basis van wetgeving. Voordat wij de verwerking starten, voeren wij een toets uit om te bepalen of wij de gegevens voor andere doelen mogen gebruiken op grond van de wet- en regelgeving.

## 8.4 Minimale gegevensverwerking

Wij mogen gegevens alleen verwerken als dit in verhouding staat tot het doel. Als we het doel waarvoor wij persoonsgegevens verwerken, zonder of met minder persoonsgegevens kunnen bereiken, dan kiezen wij daarvoor. Ook als we het doel waarvoor we persoonsgegevens verwerken op een wijze kunnen realiseren die minder inbreuk maakt op de privacy van de betrokkene, kiezen wij voor die mogelijkheid.

## 8.5 Juiste en actuele gegevens

Als provincie zorgen wij ervoor dat wij alleen persoonsgegevens verwerken die juist en actueel zijn. Wij nemen maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

### 8.6 Gegevens worden op tijd vernietigd

Wij stellen de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten die op basis van de Archiefwet 1995 zijn vastgesteld voor de provincie. Deze lijsten bepalen voor geselecteerde documenten hoelang deze bewaard moeten blijven.

Kunnen wij de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten vaststellen, dan stellen wij de bewaartermijn vast op basis van noodzakelijkheid. Wij mogen dan de persoonsgegevens niet langer bewaren dan noodzakelijk. Dit wordt beschreven en vastgelegd bij de verwerking in het verwerkingenregister. Wij bewaren gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

### 8.7 Integriteit en vertrouwelijkheid

Wij nemen passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. Wij handelen hierbij in overeenstemming met het informatiebeveiligingsbeleid. Dit beleid verplicht ons om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking. Om de vertrouwelijkheid van persoonsgegevens te waarborgen worden persoonsgegevens altijd versleuteld verstuurd en opgeslagen.

### 8.8 Privacy by Default en Privacy by Design

Wij houden bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met privacy en gegevensbescherming om zo te komen tot een optimale bescherming van persoonsgegevens. Dit uitgangspunt wordt Privacy by Design (PbD) genoemd. Wij zorgen ervoor dat we concrete maatregelen zoveel mogelijk (laten) doorvoeren in het ontwerp. Daarbij nemen we Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

### 8.9 Toegang tot gegevens

Binnen de provincie krijgen personen alleen autorisatie om persoonsgegevens te verwerken als dit voor de uitoefening van hun werkzaamheden noodzakelijk is. Wij verlenen deze bevoegdheden op grond van ons beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Wij controleren het beheer van bevoegdheden periodiek. Daarnaast hanteren wij specifieke oplossingen en toepassingen, waaronder loggegevens bijhouden. Dit doen wij om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

### 8.10 Inbreuk op persoonsgegevens (datalek)

De provincie moet passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen. Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is en waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek. Iedereen dient een (vermoeden van

een) datalek zo snel mogelijk te melden in het daarvoor bestemde meldingssysteem van de provincie. De eenheid Privacy beoordeelt of er sprake is van een datalek in de zin van de AVG en volgt het 'Protocol afhandeling datalekken'[1]. Op basis van dit protocol doet de eenheid Privacy onderzoek naar de meldingen, heeft contact met de FG en vormt indien nodig en afhankelijk van de situatie een tijdelijk datalekteam met andere benodigde expertises binnen de organisatie t.b.v. het voorgevallen datalek. De eenheid Privacy registreert datalekken, zet bevindingen om in verbeterpunten en adviseert de concerndirecteur over de afhandeling van de datalekken. Op basis van de beslissing van de concerndirecteur worden datelekken wel of niet gemeld aan de Autoriteit Persoonsgegevens en of betrokkenen. De beslissing van de concerndirecteur wordt ook verwerkt in verdere advisering aan de opgaven en opdrachten in de afhandeling van het datalek. De eenheid Privacy stemt verbeterpunten af met de betrokken opgave of opdracht geeft aan wat van de opgave of opdracht wordt verwacht en ziet toe op de opvolging hiervan.

### 8.11 Samenwerking

Als wij persoonsgegevens verwerken en daarbij het doel en de middelen bepalen, zijn wij als provincie verwerkingsverantwoordelijke. Wij schakelen soms derden in om persoonsgegevens voor ons te verwerken. Zij zijn dan verwerkers. Wij zijn in dat geval verplicht om met de verwerker een verwerkersovereenkomst af te sluiten. Deze overeenkomst zorgt dat de verwerker een vergelijkbaar beschermingsniveau biedt voor persoonsgegevens en voor de uitvoering van de rechten van betrokkenen.

In een verwerkersovereenkomst staat niet alleen welke verwerkingen er plaatsvinden en welke persoonsgegevens er worden verwerkt. Ook de afspraken over zaken als beveiliging, het al dan niet mogen inschakelen van subverwerkers en afspraken over persoonsgegevens vernietigen en over hoe om te gaan met verzoeken van betrokkenen staan hierin.

### 8.12 Samenwerkingsverbanden

Wij werken ook samen met andere (overheids-)organisaties om een taak van algemeen belang uit te voeren. Dan kan er sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). Wij spreken met deze organisaties af hoe we persoonsgegevens verwerken, wie de verwerkingsverantwoordelijke is en of er een verwerker is.

### 8.13 Doorgifte buiten de EER

Wij geven in principe geen persoonsgegevens door aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie. Behalve als we niet anders kunnen omdat er geen passend alternatief binnen de EER is. Wij kijken hierbij naar risico's op gebied van veiligheid en bescherming van persoonsgegevens, adviezen en richtlijnen van de Autoriteit Persoonsgegevens of de European Data Protection Board en een kosten-baten analyse. Wij moeten in dit geval een Data Protection Impact Assessment (DPIA) en een Data Transfer Impact Assessment (DTIA) uitvoeren.

[1] versie 1.2, vastgesteld door DT op 15 januari 2024

### 8.14 Transparantie

Natuurlijk informeren wij de betrokkenen zodat zij begrijpen waarom wij hun persoonsgegevens (moeten) verwerken. Wij wijzen hen daarbij ook op hun rechten. Wij wijken alleen van onze informatieplicht af, als de wet dat bepaalt. Voor onze eigen medewerkers staat in het interne privacy protocol welke gegevens we verwerken en waarvoor. Wij volgen ook de Wet Digitale Overheid (WDO), die de basis legt voor digitalisering van de overheid.

### 8.15 Rechten van betrokkenen

Iedereen heeft het recht om te weten welke persoonsgegevens wij over hen verzamelen en waarvoor wij die gebruiken. Betrokkenen hebben recht op inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. In de privacyverklaring op de website van de provincie worden betrokkenen geïnformeerd over verwerkingen van persoonsgegevens en wordt aangegeven hoe betrokkenen deze rechten uit kunnen oefenen.

### 8.16 Geschillenbeslechting

Als betrokkenen klachten hebben over hoe wij hun persoonsgegevens verwerken, dan kunnen zij dit melden per post, via onze website of via email (extern: fg@pzh.nl en intern via: privacy@pzh.nl). Betrokkenen kunnen ook een klacht indienen bij de Autoriteit Persoonsgegevens, als zij niet tevreden zijn over de bescherming van hun persoonsgegevens.

### 8.17 Verantwoording

Gedeputeerde Staten zijn verantwoordelijk voor hoe wij persoonsgegevens verwerken. Daar is extern en intern toezicht op. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast hebben wij een interne toezichthouder: de Functionaris voor Gegevensbescherming (FG). De FG ziet erop toe dat wij de AVG naleven. Wij geven als provincie voldoende middelen aan de FG om het toezicht adequaat uit te kunnen voeren.

### 8.18 Verwerkingen en register

Wij hebben een verwerkingsregister waar alle verwerkingen van persoonsgegevens in staan. Wij zijn als provincie verplicht om zo'n register te hebben.

Wil je binnen de provincie persoonsgegevens gaan verwerken, dan betrekt het organisatieonderdeel de eenheid Privacy in een vroeg stadium. De eenheid Privacy zorgt samen met het organisatieonderdeel dat de verwerking wordt opgenomen in het verwerkinsgregister.

Alle verwerkingen van de persoonsgegevens van collega's of verwerkingen van waarneming of controle op aanwezigheid, gedrag of prestaties van collega's (personeelsvolgsysteem) leggen we aan de OR voor ter instemming.

### 8.19 Pre-DPIA en BIO

Een pre-Data Processing Impact Assessment (pre-DPIA) is een snelle toets om te beoordelen of we persoonsgegevens gaan verwerken en hoe groot het risico van de verwerking is. De uitkomst van de pre-DPIA bepaalt of we een uitgebreide DPIA moeten uitvoeren als onderdeel van het Informatie Management (IM) proces. De pre-DPIA systematiek bestaat uit wettelijke kaders die aangeven of de gegevensverwerking voorkomt op een lijst met verwerkingen waarvoor een DPIA altijd verplicht is. Wij gebruiken hiervoor het pre-DPIA format van de eenheid Privacy.

We kunnen de pre-DPIA tegelijk met de BBN-toets afnemen, voor extra duiding. De BBN-toets is onderdeel van de Baseline Informatiebeveiliging Overheid (BIO) en is gebaseerd op de ISO 27002-standaard. Het is een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van de overheid. De toets wordt uitgevoerd door het team van Informatieveiligheid.

### 8.20 Data Protection Impact Assessment (DPIA)

Als een verwerking van persoonsgegevens mogelijk een hoog risico inhoudt voor de betrokkene, dan moeten we het effect van die verwerking beoordelen. Dit doen we door een Data Protection Impact Assessment (DPIA). We gebruiken hiervoor het DPIA-tooling van de eenheid Privacy. Blijkt uit de DPIA dat er hoge risico’s zitten aan de verwerking, dan nemen we passende maatregelen om de risico’s te verminderen. Daarnaast kan ook de FG bepalen dat de risico’s zo hoog zijn dat een DPIA noodzakelijk is. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan starten we de verwerking niet. Dan kunnen we de beoogde verwerking nog wel voorleggen aan de AP. Dit heet een voorafgaande raadpleging.

Als we een DPIA niet zelf uitvoeren, maar uitbesteden, dan gebeurt dit centraal via de eenheid Privacy.

### 8.21 Bewustwording

Met beleid en maatregelen alléén kunnen we risico’s op het terrein van verwerking van persoonsgegevens niet uitsluiten. We moeten ook het bewustzijn in de provinciale organisatie blijven aanscherpen, om veilig en verantwoord met persoonsgegevens om te gaan. Dit kan via instructies, maar altijd passend binnen de context van en bij het domein dat die persoonsgegevens verwerkt.

De eenheid Privacy zal blijvende aandacht besteden aan bewustwording binnen de organisatie. Daarnaast wordt een (verplichte) terugkerende e-learning geïmplementeerd. Dit geeft iedere medewerker voldoende basiskennis om zorgvuldig persoonsgegevens te verwerken in overeenstemming met de AVG en dit beleid.

### 8.22 Algoritmes

Sinds december 2022 hanteert de provincie een eigen algoritmeregister in aanvulling op het overkoepelende algoritmeregister van de overheid. Algoritmes zijn sets van regels en instructies die een computer geautomatiseerd volgt bij het maken van berekeningen om een probleem op te lossen of een vraag te beantwoorden. Het algoritmeregister is een overzicht van al deze algoritmes die de provincie gebruikt. In dit algoritmeregister dienen alle algoritmes op een transparante en begrijpelijke wijze te worden beschreven, inclusief de wijze hoe het algoritme tot stand komt.

Algoritmes kunnen uiteraard ook persoonsgegevens bevatten. Als de provincie algoritmische systemen wil toepassen, moet vooraf getoetst worden of hierbij aan de AVG is voldaan en de privacyrisico's in kaart zijn gebracht.

### 8.23 Artificial Intelligence (AI)

Artificial Intelligence (AI) of Kunstmatige Intelligentie is een overkoepelende term voor (zeer) geavanceerde algoritmes. Hier vallen onder andere machine learning, deep learning en neural networks onder. AI is zeer sterk in ontwikkeling en met de komst van geavanceerde chatbots en taalmodellen loopt het toezicht achter op de ontwikkelsnelheid. De chatsbots en taalmodellen zijn vrij te raadplegen en zo kunnen belangrijke documenten of transcripten inclusief persoonsgegevens worden ingevoerd.

Het is van belang dat wij zorgvuldig omgaan met die technologie en dat het bewustzijn hierover binnen de provincie wordt vergroot.

Bij de toepassing van AI-applicaties en/of platformen binnen de provincie moet vooraf worden vastgesteld of hierbij aan de AVG kan worden voldaan. De privacyrisico's moeten in kaart worden gebracht, met daarbij de juiste maatregelen om de persoonsgegevens te beschermen. Dit is ook nodig als het om een pilot, test of proefproject gaat.

### 8.24 Ethiek

Wetgeving zoals de AVG gaat over wat organisaties met data en persoonsgegevens mogen doen. Dit in tegenstelling tot ethiek dat gaat over wat organisaties met data en persoonsgegevens zouden moeten of willen doen. Als provincie moeten we rekening houden met morele waarden van medewerkers, burgers en andere externe partijen. Als een ethische, toekomstbestendige organisatie houden wij ons niet alleen aan de wet, maar houden we ook rekening met de visie van deze wetgeving. Dit doen we door wensen van betrokkenen, transparantie en privacybewustzijn mee te nemen. Zo kunnen we ethische vraagstukken over data en persoonsgegevens herkennen en kunnen we mitigerende en risicomijdende oplossingen aandragen.

Om dit de komende jaren verder te kunnen ontwikkelen werkt de eenheid Privacy nauw samen met de betrokken adviseurs en strategen binnen de provincie.