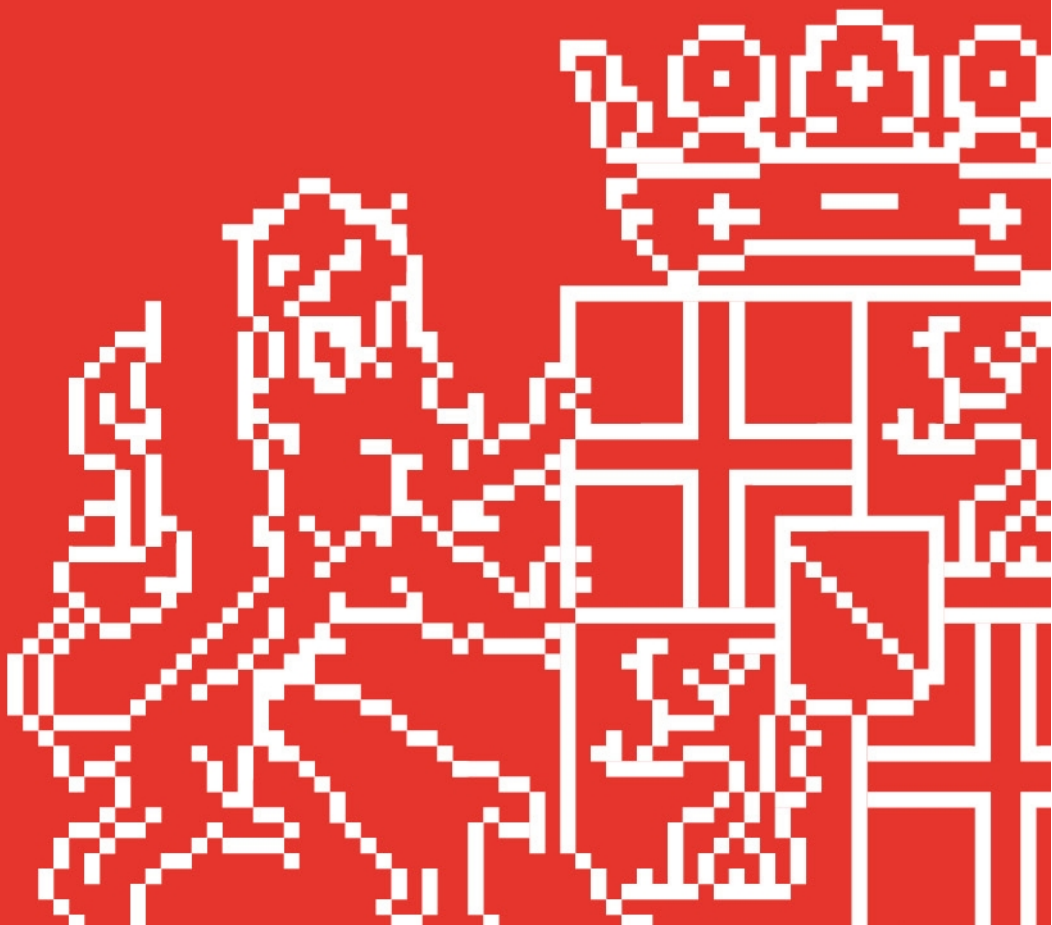
PROVINCIE UTRECHT

# PRIVACYBELEID

## PRIVACYBELEID 2021 – 2025

Publicatiedatum

Status: definitief



PROVINCIE-UTRECHT.NL

## Colofon

| | | |
|---|---|---|
| Eigenaar | : | Gedeputeerde Staten, Robert Strijk |
| Titel | : | Privacybeleid |
| Status document | : | Definitief |
| Auteur(s) | : | Ernst van Giezen en Sharda Omapersad |

## Versiebeheer

| Versie | Datum | Auteur(s) | Wijziging |
|---|---|---|---|
| 0.1 | 30-3-2020 | Ernst van Giezen | Initiële versie |
| 0.2 | 23-4-2020 | Ernst van Giezen | Feedback verwerkt |
| 0.3 | 20-10-2020 | Sharda Omapersad | Feedback verwerkt van Functionaris Gegevensbescherming |
| 1.0 | 27-11-2020 | Sharda Omapersad | Definitief |

# Inhoudsopgave

# 1. Inleiding

## 1.1 Algemeen

Dit is het privacybeleid van de provincie Utrecht. Het doel van dit beleid is om op eenduidige wijze de uitgangspunten op het gebied van privacy te communiceren. De provincie voert op uiteenlopende onderwerpen (bijvoorbeeld mobiliteit, cultuur en erfgoed, milieu en klimaat) wettelijke en bestuurlijke taken uit.[1] Voor een deel van deze taken is het noodzakelijk om Persoonsgegevens te verwerken. Dit is bijvoorbeeld het geval bij het afhandelen van een aanvraag voor een subsidie, vergunning of een ontheffing. Daarnaast verwerkt de provincie Utrecht Persoonsgegevens voor de interne bedrijfsvoering en beveiliging. Een aantal taken van de provincie Utrecht wordt uitgevoerd in samenwerkingsverbanden met andere partijen zoals verschillende gemeenten en Rijkswaterstaat.[2] Om ervoor te zorgen dat deze Verwerkingen in overeenstemming zijn met de toepasselijke wet- en regelgeving, heeft de provincie Utrecht een aantal maatregelen genomen. Gelet op de aard en hoeveelheid van de Persoonsgegevens die de provincie verwerkt, alsmede gelet op de Algemene Verordening Gegevensbescherming (hierna: AVG),[3] acht de provincie Utrecht zich gehouden deze maatregelen vast te leggen in dit privacybeleid.

Het privacybeleid wordt jaarlijks beoordeeld op actualiteit, juistheid en volledigheid en waar nodig bijgesteld. Als interne of externe wijzigingen het noodzakelijk maken om het privacybeleid te wijzigen, kunnen er tussentijdse aanpassingen plaatsvinden via hernieuwde vaststelling en publicatie door Gedeputeerde Staten.

## 1.2 Visie en kernwaarden

De provincie Utrecht heeft de afgelopen jaren aandacht en inzet gestopt in het voldoen aan privacy wet- en regelgeving. Gestreefd wordt om te groeien naar een privacy volwassenheidsniveau CIP van 2[4] op alle privacy thema´s in de periode tot en met 2022. Daarna is het de ambitie om door te groeien naar overwegend niveau 3 in 2025 .[5] Om dit te bereiken kiest de provincie Utrecht voor het uiteenzetten van haar ambitie en de uitwerking daarvan in dit privacybeleid. Op basis van dit privacybeleid zal binnen de provincie gewerkt dienen te worden aan het inbedden van een privacy compliance risicobeheersingsraamwerk dat doorlopend gemonitord wordt. Daarnaast zal er door de provincie Utrecht structureel geïnvesteerd worden in het vergroten van de bewustwording rondom privacy thema's en het verminderen of voorkomen van privacy risico's. [6]

Vanuit de provincie Utrecht is het streven dat Betrokkenen kunnen vertrouwen op een veilige Verwerking van Persoonsgegevens. Vertrouwen in de dienstverlening van de provincie is van groot belang. Het privacybeleid is gebaseerd op de volgende (bestuurlijke) uitgangspunten en provinciale kernwaarden, deze uitgangspunten versterken elkaar:

---

[1] https://www.provincie-utrecht.nl/onderwerpen.
[2] Een overzicht van alle verwerkingsdoelen en bijbehorende grondslagen zijn opgenomen in het verwerkingsregister van de Provincie Utrecht, Verwerkingsregister PU v1.5 definitief.
[3] Artikel 24 lid 2 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016.
[4] Zie 2.4 voor nadere toelichting.
[5] Programmaplan Informatieveiligheid en Privacy 2020, Stuurgroep IVenP, 17 maart 2020.
[6] FG Beoordelingsrapport, 15 juni 2020.

- Rechtmatige grondslag: de provincie Utrecht verwerkt in beginsel Persoonsgegevens op basis van grondslagen die bij de functie van overheidsorgaan horen. Dit zijn: wettelijke verplichting en een taak van algemeen belang of openbaar gezag. De voorkeur heeft om niet te verwerken op de grondslag van toestemming. Toestemming geschiedt alleen bij bijzondere gevallen, bijvoorbeeld bij experimenten en pilots.
- Burger staat centraal: de provincie Utrecht is transparant over de Verwerkingen die zij doet.
- Veiligheid: zowel bij de Verwerking van Persoonsgegevens als bij de werkomgeving van de medewerkers.
- De uitvoering van wettelijke taken van de provincie: optimale dienstverlening en privacybescherming betekenen het constant zoeken naar een evenwichtige balans.
- Ambitieus: De privacy standaard binnen de provincie Utrecht blijft groeien. De ambitie is om privacy naar een steeds hoger niveau te tillen.

## 1.3 Reikwijdte en afbakening privacy

Dit privacybeleid is van toepassing op de gehele organisatie; alle processen, onderdelen, objecten en gegevensverzamelingen van de provincie Utrecht. Het beleid ziet op alle Verwerkingen van Persoonsgegevens waarbij de provincie Utrecht zelfstandig, of gezamenlijk, Verwerkingsverantwoordelijke is. Het privacybeleid omvat de gehele 'data life cycle': van het genereren of verzamelen van Persoonsgegevens, het dagelijks gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging van Persoonsgegevens.

Dit privacybeleid is geschreven voor intern gebruik. Als derden inzicht willen in hoe de provincie Utrecht met haar gegevens omgaat, kan het privacybeleid gedeeld worden.

## 1.4 Definities

In het privacybeleid worden de volgende definities met hoofdletter gehanteerd:

*Algemene Verordening Gegevensbescherming (AVG)*
Algemene Verordening Gegevensbescherming (EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens).

*Betrokkene*
De persoon op wie de Persoonsgegevens betrekking hebben. De Betrokkene is degene van wie de Persoonsgegevens worden verwerkt.

*Datalek*
We spreken van een datalek indien vertrouwelijke informatie van de provincie Utrecht en/of Persoonsgegevens[7] zijn blootgesteld aan onrechtmatige toegang/verstrekking, diefstal, verlies, vernietiging enzovoort.[8]

*Data Protection Impact Assessment (DPIA)*
Dit is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen

[7] Zoals beschreven in paragraaf 3.2. van de Procedure met betrekking tot de afhandeling van datalekken en naleving van de meldplicht AVG, 20 juli 2020.
[8] Zoals beschreven in paragraaf 3.1. van de Procedure met betrekking tot de afhandeling van datalekken en naleving van de meldplicht AVG, 20 juli 2020.

en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is een beoordeling over het effect van de (nieuwe of aangepaste) Verwerking op de bescherming van de Persoonsgegevens en is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de Betrokkenen. De beoordeling bevat tenminste een inschatting van de risico's van de Verwerking en de vereiste beheersmaatregelen om tekortkomingen op te lossen.

*Functionaris Gegevensbescherming (FG)*
Een onafhankelijke en deskundige interne toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG).

*Persoonsgegevens*
Alle informatie over een identificeerbare of geïdentificeerde natuurlijke persoon. Het gaat hierbij om ieder gegeven dat direct gaat over een persoons ofwel te herleiden is tot een bepaalde persoon (bijvoorbeeld: naam, adres, geboortedatum). Naast "gewone" Persoonsgegevens kent de wet ook bijzondere Persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of gezondheid.

*Verwerker*
De organisatie, of persoon, die in opdracht en ten behoeve van de Verwerkingsverantwoordelijke bepaalde onderdelen van of de gehele Verwerking voor zijn rekening neemt.

*Verwerkersovereenkomst*
Een overeenkomst waarin de afspraken staan hoe een Verwerker met de Persoonsgegevens moet omgaan bij Verwerkingen in opdracht en ten behoeve van de Verwerkingsverantwoordelijke.

*Verwerking*
Een Verwerking is alles wat je met een Persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

*Verwerkingsverantwoordelijke*
De organisatie, of persoon, die bepaalt waarom de Verwerking van Persoonsgegevens plaatsvindt en vaststelt met welke middelen dat gebeurt.

*Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)*
Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

## 1.5 Wetten en regels

Het privacybeleid is in hoofdlijnen mede gebaseerd op de AVG en UAVG. In de AVG zijn de belangrijkste regels voor de rechtmatige omgang met Persoonsgegevens vastgelegd. De UAVG werkt

de nationale keuzes voor Nederland uit. De AVG regelt onder andere dat de Verwerkingsverantwoordelijke een passend privacybeleid moet opstellen.[9]

De in dit privacybeleid genoemde maatregelen zijn gebaseerd op de AVG en de UAVG. Bij de invulling en uitvoering van de maatregelen houdt de provincie Utrecht ook rekening met de beleidsregels, opinies en richtlijnen van de Autoriteit Persoonsgegevens en de het Europees Comité voor Gegevensbescherming.[10] Bescherming van Persoonsgegevens is onlosmakelijk verbonden met informatieveiligheid. Informatieveiligheid is een randvoorwaarde voor een zorgvuldige omgang met Persoonsgegevens. In de Baseline Informatiebeveiliging Overheid (hierna: BIO),[11] die van toepassing is op de provincie Utrecht, zijn normen bepaald voor informatieveiligheid.

De aard van de werkzaamheden binnen de provincie Utrecht verplicht de provincie ook aan andere wet- en regelgeving te voldoen die de Verwerking van Persoonsgegevens raken, dan wel verplichtingen opleggen. Sectorspecifieke wetgeving die van toepassing is op de Verwerking van Persoonsgegevens door de provincie Utrecht, is in Bijlage 2 opgenomen.

Mocht enige wet- of regelgeving in tegenspraak zijn of lijken met de AVG, dan wordt juridisch advies gevraagd bij team IJS (Domein Bedrijfsvoering).

### 1.6 Nadere uitwerking privacybeleid

Dit privacybeleid geldt als algemeen beleid. Voor bepaalde onderdelen stelt de provincie Utrecht, in aanvulling op het algemeen privacybeleid, specifiek uitvoeringsbeleid, nadere richtlijnen of werkwijzen op. Waar dit van toepassing is, wordt in dit privacybeleid naar die specifieke beleidsregels verwezen.

## 2. Privacybeleid

### 2.1 Doelstelling

Dit privacybeleid is een uitwerking van artikel 24 lid 2 AVG en heeft tot doel te laten zien welke maatregelen de provincie Utrecht heeft genomen om aan te tonen dat de Persoonsgegevens in overeenstemming met de toepasselijke wet- en regelgeving worden verwerkt. Daarnaast geeft het een beeld hoe de provincie Utrecht zorgt dat er transparant wordt gecommuniceerd over het gebruik van Persoonsgegevens.

### 2.2 Privacy uitgangspunten

De provincie Utrecht hanteert de volgende privacy uitgangspunten.

---

[9] Artikel 24 lid 2 AVG.

[10] Het Europees Comité voor gegevensbescherming (*European Data Protection Board* - EDPB) is een onafhankelijk Europees orgaan. De EDPB draagt bij aan de consequente toepassing van regels voor gegevensbescherming in de gehele Europese Unie (EU). Ook bevordert de EDPB de samenwerking tussen de privacytoezichthouders in de EU. Het EDPB bestaat uit vertegenwoordigers van de nationale gegevensbeschermingsautoriteiten en de Europese Toezichthouder voor gegevensbescherming (EDPS) en is de opvolger van de Werkgroep 29.

[11] https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/.

### 2.2.1 Bewaren van Persoonsgegevens

De provincie Utrecht bewaart Persoonsgegevens niet langer dan de wettelijk voorgeschreven termijnen. Als er geen sprake is van een wettelijke bewaartermijn, dan is het uitgangspunt dat Persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de uitoefening van wettelijke verplichtingen.

*Uitwerking*

De provincie Utrecht volgt de wettelijke voorgeschreven termijnen. Wanneer deze niet zijn geformuleerd door de wetgever, gelden de door de provincie vastgestelde bewaartermijnen zoals deze zijn opgenomen in het verwerkingsregister van de provincie Utrecht. De provincie Utrecht bewaart Persoonsgegevens in ieder geval in overeenstemming met selectielijsten voor archiefbescheiden van de Provinciale Organen.

Er zijn verschillende selectielijsten van toepassing op de provincie:

- Selectielijst archiefbescheiden Provinciale Organen 2005[12] en Selectielijst voor archiefbescheiden van de provinciale organen en van de Commissaris van de Koning als rijksorgaan, ontvangen of opgemaakt vanaf 1 januari 2014.[13] Deze selectielijsten worden gebruikt voor de bewaartermijn van dossiers in Documentum.
- Vernietigingslijst archiefbescheiden provinciale en interprovinciale organen 1989/1994[14] wordt gebruikt voor de archieven van de Gedeputeerde Staten en Provinciale Staten tot 2000 en het archief van de Commissaris van de Koningin tot 2014.
- Selectielijst voor archiefbescheiden van provinciale organen 2000[15] wordt gebruikt voor archieven afgesloten tussen 2000 en 2006.

Als de bewaartermijnen zijn verlopen, zal de provincie Utrecht de desbetreffende Persoonsgegevens adequaat vernietigen/verwijderen zodat deze niet langer beschikbaar zijn.

Bij verzoeken van Betrokkenen om Persoonsgegevens te verwijderen, beoordeelt de provincie Utrecht eerst of de verwijdering van deze Persoonsgegevens wettelijk is toegestaan. Indien er een wettelijke plicht op de provincie rust om de desbetreffende Persoonsgegevens te bewaren, verwijdert de provincie deze gegevens pas als de wettelijke bewaartermijn verlopen is.

### 2.2.2 Dataminimalisatie en juistheid

De provincie Utrecht verwerkt zo weinig mogelijk Persoonsgegevens. Dit betekent enkel de Persoonsgegevens die noodzakelijk zijn voor het doel van de Verwerking. De provincie Utrecht draagt zorg dat de Persoonsgegevens juist en actueel zijn.

*Uitwerking*

[12] https://wetten.overheid.nl/BWBR0019621/2006-05-10.
[13] https://www.nationaalarchief.nl/archiveren/kennisban.k/selectielijst-voor-archiefbescheiden-van-de-provinciale-organen-en-van-de.
[14] https://provisa.gbo-provincies.nl/Docs/selectielijst%201989-1994.pdf.
[15] https://wetten.overheid.nl/BWBR0011749/2000-11-26/0/informatie.

De juistheid van Persoonsgegevens binnen de processen van de provincie Utrecht is geborgd. Mochten Betrokkenen van mening zijn dat hun Persoonsgegevens niet juist zijn, kunnen zij een verzoek indienen deze te wijzigen, blokkeren of verwijderen. Dit is geregeld in de **Procedure rechten van betrokkenen.**[16] Daarnaast is in het register van verwerkingsactiviteiten[17] vastgelegd per Verwerking welke Persoonsgegevens door de provincie worden verwerkt.

### 2.2.3 Delen met derden

Wanneer er sprake is van structurele of gevoelige gegevensuitwisseling met derde partijen, worden er afspraken gemaakt over de gegevensuitwisseling.[18] Deze afspraken voldoen tenminste aan de AVG en worden vastgelegd in een onderlinge regeling, een gegevensuitwisselingsovereenkomst of een Verwerkersovereenkomst.

*Uitwerking*

Er is een Model **verwerkersovereenkomst**[19] aanwezig dat inhoudelijk voldoet aan de eisen die de AVG daaraan stelt. De provincie Utrecht houdt de Verwerkers waarmee een Verwerkersovereenkomst is afgesloten bij in het register van verwerkingsactiviteiten. De ondertekende versies van de Verwerkersovereenkomsten behoren bij de proceseigenaren te zijn gearchiveerd. Voor onderlinge regelingen of gegevensuitwisselingsovereenkomsten kan contact worden opgenomen met de Privacy Officers.

### 2.2.4 Doelbinding

Provincie Utrecht verzamelt alleen Persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Bij de uitwerking wordt rekening gehouden met de eisen van proportionaliteit en subsidiariteit. Dit betekent dat de gegevensverwerking in relatie moet staan tot het doel en wanneer er sprake is van een inbreuk op de privacy, dit op de minst ingrijpende manier plaatsvindt. De Persoonsgegevens worden alleen voor een ander doel gebruikt als dat doel niet onverenigbaar is met de oorspronkelijke verzameldoeleinden.

*Uitwerking*

De provincie Utrecht verwerkt alleen Persoonsgegevens als daarvoor een doel is vastgesteld. Per individuele Verwerking moet het doel uitdrukkelijk omschreven en gerechtvaardigd zijn. Voor de uitvoering van diverse provinciale taken zijn de doelen voor het verwerken in de wet vastgelegd, net als de Persoonsgegevens die gevraagd en verwerkt mogen worden. Er wordt een register van verwerkingsactiviteiten[20] bijgehouden waarin per Verwerking de doeleinden worden vermeld. Er wordt geborgd dat bij wijzigingen in de Verwerkingen, dan wel de doeleinden, deze beoordeeld en gewijzigd worden in het register van verwerkingsactiviteiten.

---

[16] Procedure verzoeken Rechten Betrokkenen (september 2020).
[17] Verwerkingsregister PU v1.5 definitief.
[18] Stroomschema is een verwerkersovereenkomst nodig, Procesbeschrijving aangaan verwerkersovereenkomst, Procesbeschrijving beheer en beëindiging verwerkersovereenkomst (https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_2).
[19] Model verwerkersovereenkomst PU (https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_2).
[20] Verwerkingsregister PU v1.5 definitief.

### 2.2.5 Integriteit en vertrouwelijkheid

De provincie Utrecht gaat zorgvuldig om met de haar toevertrouwde Persoonsgegevens en behandelt deze vertrouwelijk. De provincie neemt passende technische en organisatorische beveiligingsmaatregelen om Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, verlies of wijziging, ongeautoriseerde openbaarmaking, misbruik of anderszins Verwerking in strijd met de wet.

*Uitwerking*

De volgende maatregelen zijn genomen om Persoonsgegevens te beschermen:

- Medewerkers van de provincie Utrecht zijn zich bewust van de vertrouwelijkheid van Persoonsgegevens en handelen hiernaar;
- Er is een **Informatiebeveiligingsbeleid;**[21]
- Een vaste DPIA-procedure is **aanwezig;**[22]
- Er is een **procedure Datalekken.**[23]

### 2.2.6 Rechten van Betrokkenen

De provincie Utrecht ondersteunt Betrokkenen in het uitoefenen van hun rechten en draagt er zorg voor dat zij op een laagdrempelige manier aanspraak op hun rechten kunnen maken.

*Uitwerking*

Er is een **Procedure rechten van betrokkenen**[24] aanwezig waarin een tijdige afhandeling van verzoeken van Betrokkenen wordt gewaarborgd.

### 2.2.7 Rechtmatigheid en transparantie

Uitgangspunt is dat Persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke, transparante en zorgvuldige wijze worden verwerkt. De provincie Utrecht verwerkt alleen Persoonsgegevens op basis van een gerechtvaardigde verwerkingsgrondslag.

*Uitwerking*

De provincie Utrecht heeft procedures en protocollen opgesteld om te waarborgen dat haar medewerkers weten hoe zij om moeten gaan met Persoonsgegevens. Een overzicht van deze procedures en protocollen is opgenomen in Bijlage 1. Alle medewerkers weten dat zij uitsluitend Persoonsgegevens mogen verwerken als hiervoor een wettelijke grondslag is.

De rechtmatigheid houdt in dat de provincie Utrecht alleen Persoonsgegevens verwerkt als hier een wettelijke grondslag voor is. De Verwerking wordt vermeld in het register van verwerkingsactiviteiten.[25]

---

[21] Informatiebeveiligingsbeleid provincie Utrecht 2020-2022 https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_6.
[22] https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_4.
[23] Procedure datalekken (juli 2020) https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_7.
[24] Procedure verzoeken Rechten Betrokkenen (september 2020).
[25] Verwerkingsregister PU v1.5 definitief.

De provincie Utrecht draagt zorg dat, indien hier om wordt verzocht, de Betrokkene informatie krijgt omtrent de verwerkte Persoonsgegevens. Het beginsel van transparantie zorgt ervoor dat bij het verzamelen van Persoonsgegevens de Betrokkenen de volgens de wet vereiste informatie ontvangen in de vorm van een privacyverklaring.

## 2.3 Verplichtingen AVG

### 2.3.1 Register van verwerkingsactiviteiten

Om invulling te kunnen geven aan de verplichtingen die voortvloeien uit het verwerken van Persoonsgegevens, heeft de provincie Utrecht een **verwerkingsregister**[26] opgesteld, zoals genoemd in artikel 30 AVG. Dit verwerkingsregister bevat:

- De naam en contactgegevens van de provincie, de FG en eventuele andere organisaties waarmee de provincie Utrecht gezamenlijk Verwerkingsverantwoordelijke is;
- De doelen van de Verwerkingen;
- Een beschrijving van de categorieën van Betrokkenen en de categorieën Persoonsgegevens die de provincie Utrecht verwerkt;
- Een beschrijving van de ontvangers van de Persoonsgegevens;
- Indien van toepassing, een beschrijving van het delen van Persoonsgegevens aan derde landen;
- De bewaartermijnen;
- Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

De Privacy Officers beheren het register van verwerkingsactiviteiten.[27] Proceseigenaren zijn verantwoordelijk voor het opnemen van nieuwe Verwerkingen in het register van verwerkingsactiviteiten. Zij worden hierbij geadviseerd door de Privacy Officers. De FG controleert of het register van verwerkingsactiviteiten volledig en up-to-date is. In het **beheerdocument verwerkingsregister**[28] zijn de rollen en verantwoordelijkheden ten aanzien van het beheer van het register van verwerkingsactiviteiten vastgelegd. Het register van verwerkingsactiviteiten wordt periodiek geactualiseerd. Eén keer per jaar richten de Privacy Officers zich tot de proceseigenaren met het verzoek om het register van verwerkingsactiviteiten te controleren op actualiteit en juistheden.

### 2.3.2 Data Protection Impact Assessment

Voor de provincie Utrecht geldt dat voor een nieuwe Verwerking of een wijziging in een bestaande Verwerking een **Business Impact Analyse (BIA)**[29] uitgevoerd dient te worden. Een BIA wordt door een Information Security Officer en een Privacy Officer samen met de proceseigenaar uitgevoerd. Aan de hand van de uitgevoerde BIA worden voor zowel informatiebeveiliging als privacy, een risico-inventarisatie uitgevoerd als er aanleiding toe is. Op basis van de uitgevoerde BIA wordt bepaald of voor een afzonderlijke Verwerking een hoog risico bestaat en een DPIA noodzakelijk is.

[26] Verwerkingsregister PU v1.5 definitief.
[27] Verwerkingsregister PU v1.5 definitief
[28] Beheer verwerkingsregister V1.0 (17-3-2020 vastgesteld door stuurgroep IV&P).
[29] BIA template v0.9.

Indien er sprake is van Verwerkingen met een hoog privacyrisico voor Betrokkenen, dient er voorafgaand aan die verwerking een Data Protection Impact Assessment (DPIA) uitgevoerd te worden.[30] Een DPIA geeft inzicht in welke maatregelen getroffen moeten worden om het risico te verkleinen naar een minimaal en acceptabel niveau.

De provincie Utrecht beschikt over een **standaard model DPIA**[31] voor de uitvoering van een DPIA. Proceseigenaren zijn verantwoordelijk voor de uitvoering van een DPIA voor een Verwerking met een hoog privacyrisico. Privacy Officers en Information Security Officers ondersteunen en adviseren bij de uitvoering hiervan.[32] De FG geeft advies over de uitgevoerde DPIA op grond van art. 39 lid 1 onder c AVG en ondertekent de DPIA. De Privacy Officers houden een register bij van uitgevoerde DPIA´s en monitoren de voortgang van te implementeren beheersmaatregelen en rapporteren daarover aan GS.

Processen kunnen regelmatig worden aangepast. Dit kan ook effect hebben op de Verwerking van Persoonsgegevens. Als er een wijziging in het proces wordt doorgevoerd is het noodzakelijk om een eerder uitgevoerde DPIA te herzien en te kijken of de wijziging ook nieuwe risico's met zich meebrengt. Ook indien er geen proceswijzigingen worden doorgevoerd, is het noodzakelijk de uitgevoerde DPIA periodiek te herzien. De proceseigenaren zijn verantwoordelijk zijn voor de actualisering na drie jaar van de DPIA.

Hiervan kan worden afgeweken indien blijkt dat het restrisico hoog is. Aan de hand van het netto risico wordt bepaald of de periodiciteit aangepast moet worden, de Privacy Officer en de FG adviseren over de eventuele verkorting van de periodiciteit in samenspraak.

### 2.3.3 Privacy by Design en Privacy by Default

Op grond van artikel 25 AVG dient bij de Verwerking van Persoonsgegevens *Privacy by Design* en *Privacy by Default* toegepast te worden.

*Privacy by Design* houdt in dat er al bij het ontwerpen van producten en diensten voor wordt gezorgd dat Persoonsgegevens goed worden beschermd. Bij de inrichting van het proces en/of bouw van het systeem wordt bijvoorbeeld gekeken naar de benodigde technische en organisatorische maatregelen om deze Persoonsgegevens te beschermen. Ook dataminimalisatie is een uitgangspunt wat gehanteerd kan worden.

In het **Informatiebeveiligingsbeleid**[33] komt het principe van *Privacy by Design* terug. Daarin wordt aangegeven dat privacy aan het begin van de uitvoer van projecten wordt meegenomen. Rollen die hierop toezien zijn de Information Security Officer en de FG. Het Programmaplan Informatieveiligheid en Privacy 2020[34] geeft aan dat de Corporate Information Security Officer op dit moment met een achterstand te maken heeft wat betreft het toezicht op projecten en programma's, wat betekent dat er minder controle is op de implementatie van *Privacy by Design* bij de start van

[30] Artikel 35 AVG.
[31] Vragenlijst template DPIA PU v2.9, https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_5.
[32] Procesbeschrijving uitvoeren DPIA versie 1.0 zie https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_4.
[33] Informatiebeveiligingsbeleid provincie Utrecht 2020 – 2022 Zie https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_5.
[34] Programmaplan Informatieveiligheid en Privacy, Stuurgroep IVenP, 17 maart 2020.

projecten en programma's. De provincie Utrecht heeft op dit gebied nog stappen te maken wat betreft de awareness op en de implementatie van *Privacy by Design* bij de start van projecten.

*Privacy by Default* houdt in dat de standaardinstellingen van een programma standaard ingesteld dienen te worden op de meest privacy vriendelijke manier.

Zoals beschreven in 2.3.2 geldt voor de provincie Utrecht dat voor een nieuwe Verwerking of een wijziging in een bestaande Verwerking een BIA uitgevoerd dient te worden. Bij het uitvoeren van een BIA, en in sommige gevallen een aanvullende DPIA, worden de voor *Privacy by Design* en *Privacy by Default* noodzakelijke aspecten (bijvoorbeeld dataminimalisatie en bewaartermijnen) meegenomen in de voorgenomen Verwerking. Op deze manier wordt geborgd dat nieuwe Verwerkingen conform de normen van *Privacy by Design* en *Privacy by Default* worden ingericht.

### 2.3.4 Datalekken

Er wordt gesproken van een Datalek indien vertrouwelijke informatie van de provincie Utrecht en/of Persoonsgegevens[35] zijn blootgesteld aan onrechtmatige toegang/verstrekking, diefstal, verlies, vernietiging enzovoort.[36]

Wanneer een Datalek heeft plaatsgevonden en het waarschijnlijk is dat dit Datalek leidt tot een risico voor de rechten en vrijheden van Betrokkenen, dient dit te worden gemeld bij de toezichthouder, de Autoriteit Persoonsgegevens (hierna: AP). Deze melding dient onmiddellijk, maar uiterlijk binnen 72 uur nadat er kennis is genomen van het Datalek, te worden gemeld bij de AP. Indien dit later dan 72 uur is, wordt er een motivering voor de vertraging bij de melding gevoegd. Indien het Datalek een hoog risico met zich meebrengt voor Betrokkenen, meldt de provincie Utrecht dit ook aan de Betrokkenen.

De provincie Utrecht heeft een vastgestelde **procedure Datalekken[37]** waarin is beschreven op welke wijze Datalekken binnen de provincie Utrecht worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft. In deze procedure is ook opgenomen in welke gevallen en op welke manier de toezichthouder en/of de Betrokkenen over het Datalek worden geïnformeerd. Voor medewerkers is informatie over het melden van Datalekken beschikbaar op Atrium.[38] Daarnaast is het melden van Datalekken een terugkerend onderwerp bij awareness activiteiten.

Tevens is er een intern **register van datalekken[39]** waarin alle geconstateerde beveiligingsincidenten worden geregistreerd. Hierin wordt vastgelegd of het beveiligingsincident heeft geleid tot een

[35] Zoals beschreven in paragraaf 3.2. van de Procedure met betrekking tot de afhandeling van datalekken en naleving van de meldplicht AVG, 20 juli 2020, https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_7.

[36] Zoals beschreven in paragraaf 3.1. van de Procedure met betrekking tot de afhandeling van datalekken en naleving van de meldplicht AVG, 20 juli 2020, https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_7.

[37] Procedure met betrekking tot de afhandeling van datalekken en naleving van de meldplicht AVG, 20 juli 2020, https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_7.

[38] Https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_7.

[39] Datalekken en incidentenregister.

Datalek en indien dat het geval is, het Datalek ook is gemeld bij de toezichthouder en/of de Betrokkenen. Daarnaast wordt ieder Datalek geëvalueerd om toekomstige Datalekken te voorkomen.[40]

### 2.3.5 FG

De provincie Utrecht is een overheidsinstantie die structureel en op grote schaal Persoonsgegevens verwerkt, waaronder bijzondere Persoonsgegevens. Het is in dit geval een wettelijke verplichting een Functionaris Gegevensbescherming (FG) aan te stellen. De provincie Utrecht heeft een FG in dienst. Contactgegevens van de FG staan vermeld op de website van de provincie Utrecht.

De FG is een onafhankelijke toezichthouder die gevraagd en ongevraagd advies geeft op het gebied van de AVG. Om de FG in staat te stellen deze adviesrol te vervullen wordt alle relevante informatie tijdig met de FG gedeeld, zodat hij/zij passend advies kan verlenen. Advisering door de FG is niet vrijblijvend. Op een door de FG uitgebracht advies wordt binnen 5 werkdagen een reactie gegeven door de geadresseerde van het advies. Wanneer het advies van de FG niet wordt gevolgd, laat de geadresseerde van het advies dit met redenen omkleed weten aan de FG. De FG krijgt de kans om zijn/haar afwijkende mening duidelijk te maken aan de verwerkingsverantwoordelijke.

De FG maakt jaarlijks een FG toezichtplan, voert dit uit en rapporteert periodiek over de naleving van privacy wet- en regelgeving binnen de provincie Utrecht en over uitgevoerde onderzoeken. De FG rapporteert een keer per jaar in een jaarverslag en een keer per jaar in een tussentijds verslag.

De FG heeft onder meer de volgende wettelijke taken:

- Informatievoorziening;
- Toezicht op de implementatie van de privacy wet- en regelgeving;
- Contactpersoon voor de Autoriteit Persoonsgegevens;
- Periodieke verslaglegging aan Gedeputeerde Staten over de uitvoering van zijn taken;
- Het zorg dragen voor een juiste afwikkeling van de vragen of klachten van Betrokkenen;
- Adviseren bij en toezien op de uitvoering van DPIA's en bij beoordeling van Datalekken.

### 2.3.6 Beveiliging

Op grond van de AVG dienen organisaties passende technische en organisatorische maatregelen te nemen om de Persoonsgegevens die zij verwerkt, te beveiligen. De provincie Utrecht heeft een **Informatiebeveiligingsbeleid**[41] opgesteld waarin is beschreven op welke wijze invulling is gegeven aan de passende beveiliging van Persoonsgegevens. Tevens is er een Corporate Information Security Officer (hierna: CISO) een Technical Information Security Officer (hierna: TISO) en zijn er twee Information Security Officers aangesteld.

[40] Zoals beschreven in paragraaf 5.9 van de Procedure met betrekking tot de afhandeling van datalekken en naleving van de meldplicht AVG, 20 juli 2020, https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_7.

[41] Informatiebeveiligingsbeleid provincie Utrecht 2020 – 2022 Zie https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_5.

### 2.3.7. Rechten van Betrokkenen

Betrokkenen van wie de provincie Utrecht Persoonsgegevens verwerkt, hebben volgens de wet bepaalde rechten waarmee zij controle kunnen uitoefenen op de Verwerking van hun Persoonsgegevens. De provincie Utrecht onderschrijft deze rechten en zal ook aan de verzoeken van Betrokkenen omtrent deze rechten voldoen. In de privacyverklaring[42] van de provincie Utrecht staan de volgende rechten:

- U heeft recht op inzage van de Persoonsgegevens die wij van u verwerken.
- U heeft recht op informatie over de wijze waarop wij uw Persoonsgegevens verwerken.
- U heeft recht op correctie of aanvulling van uw Persoonsgegevens.
- U heeft het recht om uw Persoonsgegevens te laten verwijderen.
- U heeft het recht om minder Persoonsgegevens te laten verwerken.
- U kunt bezwaar maken tegen de Verwerking van uw Persoonsgegevens.
- U heeft het recht ons te verzoeken uw Persoonsgegevens in een gestructureerde, gangbare en machine-leesbare vorm aan u over te dragen.
- U kunt bezwaar maken tegen geautomatiseerde individuele besluitvorming.

De provincie Utrecht heeft een vastgestelde **Procedure rechten van betrokkenen[43]** waarin is beschreven op welke wijze verzoeken van Betrokkenen binnen de provincie Utrecht worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft. De procedure waarborgt een tijdige afhandeling van de verzoeken. Om gebruik te maken van zijn of haar rechten kan Betrokkene een verzoek indienen. De provincie heeft vanaf ontvangst van het verzoek vier weken de tijd om het verzoek te behandelen. Het verzoek is via het e-mailadres privacy@provincie-utrecht.nl in te dienen.

### 2.3.8. Transparante informatie

In de AVG is opgenomen dat Persoonsgegevens verwerkt moeten worden op een manier die transparant is voor de Betrokkenen. Voor de Betrokkene moet transparant zijn of en in hoeverre zijn Persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt.

De provincie Utrecht dient Betrokkenen bij de verkrijging van de Persoonsgegevens te informeren over de Verwerking van de Persoonsgegevens. De provincie Utrecht heeft een **Privacy verklaring[44]** op haar website waarin Betrokkenen worden geïnformeerd over de Verwerking van Persoonsgegevens door de provincie Utrecht. Aanvullend op deze algemene berichtgeving worden Betrokkenen bij specifieke processen, waar mogelijk en noodzakelijk, aanvullend geïnformeerd over de betreffende gegevensverwerking.

### 2.3.9. Privacyovereenkomsten en doorgiften

Als de provincie Utrecht de Verwerking van Persoonsgegevens uitbesteedt aan een andere partij zoals bijvoorbeeld een Verwerker, dan moet de provincie met die partij afspraken maken over de wijze waarop die partij de Persoonsgegevens mag verwerken en welke verplichtingen die partij dan

[42] https://www.provincie-utrecht.nl/privacy.
[43] Procedure verzoeken Rechten Betrokkenen (september 2020).
[44] https://www.provincie-utrecht.nl/privacy.

heeft. Deze afspraken moeten worden vastgelegd in een privacyovereenkomst tussen provincie Utrecht en de partij.[45] De vastlegging kan geschieden in een verwerkersovereenkomst, onderlinge regeling of een gegevensuitwisselingsovereenkomst. De provincie Utrecht heeft een eigen model **verwerkersovereenkomst**[46] dat inhoudelijk voldoet aan de eisen die de AVG daaraan stelt. Dit model is, met een extra toelichting, gepubliceerd op Atrium. In overleg met partijen kan ook een ander model gehanteerd worden, mits dit ook voldoet aan de gestelde eisen op grond van de AVG. Dit wordt beoordeeld door de Privacy Officers.

Het kan zijn dat de provincie Utrecht met een andere partij gezamenlijk Verwerkingsverantwoordelijke is. In dat geval sluit de provincie Utrecht een onderlinge regeling af, waarin minimaal de gemeenschappelijke en per partij specifieke verantwoordelijkheden en plichten zijn opgenomen. Mocht er ook geen sprake zijn van een gezamenlijke Verwerkingsverantwoordelijkheid, dan kunnen de Privacy Officers en FG adviseren om de verhoudingen ten aanzien van de verantwoordelijkheden van privacy- en gegevensbescherming van een bepaalde samenwerking vast te leggen in een gegevensuitwisselingsovereenkomst.

De provincie Utrecht maakt in het register van verwerkingsactiviteiten per Verwerking inzichtelijk hoe andere partijen gekwalificeerd dienen te worden zoals of er sprake is van een ingeschakelde Verwerker en of hier een Verwerkersovereenkomst mee is aangegaan. Bijzondere privacyovereenkomsten dienen voor advies aan de FG te worden voorgelegd.

Met betrekking tot doorgifte hanteert de provincie het uitgangspunt dat Persoonsgegevens niet worden doorgegeven aan een bedrijf of vestiging in een land buiten de Europese Economische Ruimte (EER), tenzij deze doorgifte aantoonbaar rechtmatig is.

## 2.4 Risico's

Het privacy control framework van de provincie Utrecht is vormgegeven door de Privacy baseline en het Privacy volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacybescherming (CIP).[47] Dit dient als het beoordelingskader voor het waarborgen van privacy compliance binnen de provincie Utrecht. De Privacy baseline en het Privacy volwassenheidsmodel van het CIP geven invulling aan het normenkader voor het duiden van privacyrisico's en de daarbij behorende beheersmaatregelen binnen de provincie Utrecht.

Op basis van de Privacy baseline en het Privacy volwassenheidsmodel zal de provincie Utrecht kerncontrolepunten en bijbehorende werkprogramma's vaststellen.

## 2.5 Verantwoordelijken

Het college van Gedeputeerde Staten is verantwoordelijk voor het naleven van de uitgangspunten uit de privacy wet- en regelgeving en de kaders voor het verantwoord omgaan met Persoonsgegevens. Dat de uitgangspunten en kaders ook daadwerkelijk worden gehanteerd, dient Gedeputeerde Staten

[45] Artikel 28 lid 3 AVG.
[46] Model verwerkersovereenkomst PU, https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_2.
[47] www.cip-overheid.nl.

te kunnen aantonen. Over de uitvoering van het privacybeleid legt Gedeputeerde Staten verantwoording af aan Provinciale Staten.

*Het college van Gedeputeerde Staten:*

- Is eindverantwoordelijk voor het op een behoorlijke en zorgvuldige manier verwerken van Persoonsgegevens door de provincie Utrecht;
- Dient aan te kunnen tonen dat Persoonsgegevens door de provincie Utrecht in overeenstemming met privacy wet- en regelgeving worden verwerkt;
- Laat daartoe kaders opstellen voor de bescherming van de privacy op basis van wet- en regelgeving;
- Wijst uit haar midden een portefeuillehouder privacy aan die bestuurlijk verantwoordelijk is voor de uitvoering van het provinciaal privacybeleid en voor de controle op de naleving hiervan.

Het verantwoord omgaan met Persoonsgegevens brengt echter niet alleen verantwoordelijkheden met zich mee voor Gedeputeerde Staten, maar ook voor directie, management en uiteindelijk iedere medewerker van de provincie Utrecht.

*De directie:*

- Is verantwoordelijk voor de uitvoering van en sturing op de beleidskaders (waarbij wordt gestuurd op concernrisico's);
- Zorgt dat de getroffen maatregelen voldoende bescherming bieden om de privacy van Betrokkenen te beschermen;
- Zorgt dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van Persoonsgegevens;
- Beoordeelt periodiek (de uitwerking van) het privacybeleid op basis van de evaluatie en aanpassingen van het privacybeleid en -plan.

*De domeinmanagers:*

- Stellen, indien nodig, voor het betreffende organisatieonderdeel specifieke privacykaders op en leggen dit voor aan de directie ter vaststelling. Deze specifieke kaders dienen te passen binnen het overkoepelende beleid en maakt daar onderdeel van uit;
- Zorgen voor naleving van wet-, regelgeving, beleid en de bijbehorende werkinstructies;
- Zorgen dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van Persoonsgegevens;
- Maken afspraken met andere organisatieonderdelen over het borgen van de privacy in geval van informatie die stroomt tussen verschillende organisatieonderdelen;
- Kunnen hun verantwoordelijkheden op onderdelen mandateren aan teamleiders, programmamanagers, projectleiders of andere medewerkers.

*De Privacy Officers*

- Zorgen dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van Persoonsgegevens;

- Stellen indien nodig in het kader van de bescherming van Persoonsgegevens centraal privacybeleid, richtlijnen, procedures en instructies op namens en ter vaststelling door Gedeputeerde Staten (de meeste stukken worden op een lager niveau vastgesteld door het lijnmanagement);
- Adviseren lijnmanagement over het opstellen van onder andere privacyovereenkomsten, het adviseren over het aanleveren van informatie voor het bijhouden van het verwerkingsregister, het uitvoeren van een DPIA en overige advisering in het kader van de toepassing van privacy wet- en regelgeving;
- Adviseren het lijnmanagement bij datalekken (beoordelen, adviseren met betrekking tot maatregelen en melden bij de AP);
- Verzorgen interne voorlichtingsbijeenkomsten en gerichte trainingen voor specifieke doelgroepen.

*Alle medewerkers*

- Zijn vanuit hun eigen functie of rol verantwoordelijk voor de bescherming van de privacy van Betrokkenen en gehouden aan geheimhouding en naleving van de toepasselijke wet- en regelgeving (inclusief de interne beleidsregels van de provincie). Dat betekent dat iedereen bijdraagt aan en medeverantwoordelijkheid draagt voor een rechtmatige, behoorlijke en transparante Verwerking van Persoonsgegevens.

De taken, verantwoordelijkheden en bevoegdheden van de teamleiders/opgavemanagers en de FG (zie ook 2.3.5) zijn vastgelegd in het **Statuut Gegevensbescherming.**[48]

De concretisering van de privacy organisatie binnen de provincie Utrecht is gevisualiseerd in de RASCI-matrix, zoals opgenomen in Bijlage 3. In het Programmaplan Informatieveiligheid en Privacy 2020 is de rolverdeling binnen de privacy organisatie uiteengezet.[49]

## 2.6 Uitwerking en evaluatie

Dit privacybeleid is ontwikkeld door een cyclisch proces van voorbereiding, ontwikkeling, goedkeuring en evaluatie (Plan-Do-Check-Act). Privacy en gegevensbescherming kunnen door hun dynamiek en toenemend belang op deze wijze effectief worden geborgd.

Dit privacybeleid dient door het lijnmanagement uitgewerkt te worden in specifiek uitvoeringsbeleid, nadere richtlijnen en/of werkinstructies. Minimaal één keer per jaar, of eerder indien daar aanleiding toe is, wordt dit privacybeleid geëvalueerd en indien nodig aangepast. Specifiek uitvoeringsbeleid, richtlijnen en werkinstructies zoals het privacy of het cookie statement van de provincie, worden eveneens minimaal jaarlijks door het verantwoordelijke lijnmanagement geëvalueerd. Hierover dient door het lijnmanagement te worden gerapporteerd.

[48] Besluit van Gedeputeerde Staten van Utrecht van 2 juli 2019, nr.81F20568, tot vaststelling van een statuut gegevensbescherming.

[49] Programmaplan Informatieveiligheid en Privacy 2020, Stuurgroep IVenP, 17 maart 2020.

De FG schrijft kwartaalrapportages voor de directie op basis van het geschreven toezichtplan. Deze rapportages richten zich op specifieke aandachtspunten en het algemene volwassenheidsniveau van de provincie Utrecht. Een keer per jaar brengt de FG een beoordelingsrapport uit en tweemaal per jaar informeert de FG Gedeputeerde Staten door middel van een C-stuk.

## 2.7 Bewustwording

De provincie Utrecht borgt dat alle medewerkers een hoog niveau van bewustwording hebben op het gebied van privacy. In het kader daarvan is het lijnmanagement verantwoordelijk voor informerende en voorlichtende activiteiten op het gebied van privacy waarbij in ieder geval de meldplicht datalekken een terugkerend onderwerp is. Medewerkers van alle lagen worden betrokken bij actuele privacy-issues en Datalekken om bewustwording te borgen. Verder heeft de provincie ook eigen **richtsnoeren.**[50] In deze richtsnoeren, die zien op veel binnen de provincie Utrecht voorkomende Verwerkingen, worden *do's and don'ts* voor medewerkers van de provincie op laagdrempelige wijze nader uitgewerkt en gepubliceerd op Atrium (het intranet van de provincie Utrecht). Deze richtsnoeren kunnen in de toekomst verder worden uitgebreid en worden jaarlijks geactualiseerd.

## 2.8 Privacybeleid HRO

De in dit privacy beleid onder 2.2 en 2.3 genoemde privacy uitgangspunten en verplichtingen zijn ook van toepassing op de Provincie Utrecht als werkgever ten aanzien van haar werknemers en zullen door HRO in specifiek beleid nader worden uitgewerkt.

## 2.9 Inwerkingtreding

Het privacybeleid treedt in werking per …. (p.m.)

[50] Richtlijn IBP 1 - fotograferen en film
Richtlijn IBP 2 - Checklist organiseren bijeenkomsten
Richtlijn IBP 3 - Anonimiseren bij publicatie
Richtlijn IBP 4 - BSN nummer en kopie van paspoort
Richtlijn IBP 5 - regels en classificaties omtrent documenten
Richtlijn IBP 6 - Wachtwoord
Richtlijn IBP 7 – Stroomschema opnemen gesprekken in Teams
*https://socialintranet.provincie-utrecht.nl/programma-s-en-projecten/informatieveiligheid-en-privacy#toc_4.*

## Bijlage 1 Procedures en Protocollen

**Algemeen**

Statuut Gegevensbescherming

Privacy beleid

Privacy Statement (extern)

Protocol controle en onderzoek bedrijfsmiddelen

Procedure Datalekken

Infosheet datalekken (verkorte versie van de procedure)

Procedure rechten van betrokkenen

**Richtlijnen IV&P**

Richtlijn IBP 1 - fotograferen en film

Richtlijn IBP 2 - Checklist organiseren bijeenkomsten

Richtlijn IBP 3 - Anonimiseren bij publicatie

Richtlijn IBP 4 – BSN nummers en Kopieën paspoorten

Richtlijn IBP 5 - Regels en classificaties omtrent documenten

Richtlijn IBP 6 – Wachtwoord

Richtlijn IBP 7 – Stroomschema opnemen gesprekken in Teams

**Verwerkersovereenkomst**

Model verwerkersovereenkomst PU

Model samenwerkingsprotocol AVG - PU

stroomschema 'is een verwerkersovereenkomst nodig' v1.0

Procesbeschrijving aangaan verwerkersovereenkomst

Procesbeschrijving beheer en beëindiging vwo

**DPIA**

Template DPIA PU v2.0

stroomschema 'is een DPIA nodig' versie 1.0

Procesbeschrijving uitvoeren DPIA versie 1.0

**Verwerkingsregister**

Verwerkingsregister PU v1.5 definitief

Beheerdocument verwerkingsregister V1.0 (17-3-2020 vastgesteld door stuurgroep IV&P)

## Bijlage 2 Sectorspecifieke wet- en regelgeving

De provincie Utrecht valt ten aanzien van de verwerking van persoonsgegevens ook onder de werking van de volgende sectorspecifieke wet- en regelgeving:

- **Telecommunicatiewet**
    - *Artikel 11.7 a bepaalt in aanvulling op de AVG regels voor het gebruik van cookies. Overeenkomstig de Telecommunicatiewet vraagt de PU bezoekers van haar website toestemming voor het gebruik van cookies.*

*Op basis hiervan toont de provincie een melding op haar website waarbij bezoekers van de website worden geïnformeerd over het gebruik van cookies en hen een keuze wordt geboden om te bepalen welke cookies zij wel en niet accepteren. In aanvulling op deze melding is er een cookieverklaring waarin nadere informatie over het gebruik van de cookies wordt verstrekt.*

## Bijlage 3 RASCI-matrix

| Task | GS | Directie | Domeinmanager | Privacy Officer | Medewerkers | FG |
|---|---|---|---|---|---|---|
| Beleid | | | | | | |
| Privacybeleid/Privacyrichtlijnen/Standaarddocumenten en privacygerelateerde procesbeschrijvingen | A | R | R | S | I | I |
| Training en Awareness | A | R | R | S | I | S |
| Rapportages | | | | | | |
| Rapportage over de uitvoering van processen | A | R | R | S | I | I |
| Rapportage over naleving van de AVG | I | I | ! | C | | A |
| Rechten van betrokkenen | | | | | | |
| Proces, vastlegging en rapportage | A | R | R | S | | I |
| Aanleveren, verwijderen, corrigeren informatie | A | R | R | C | S | I |
| Register van verwerkingen | | | | | | |
| Beheer en onderhoud en rapportage register | A | R | R | S | | I |
| Actueel houden informatie verwerkingen | A | R | R | R | S | I |
| DPIA | | | | | | |
| Beheer en onderhoud van DPIA documentatie en standaardmodellen | A | R | R | S | I | I |
| Uitvoeren DPIA voor hoog risico processen | A | R | R | C | S | C |
| Datalekken | | | | | | |
| Beheer en onderhoud van documentatie, vastlegging incidenten, rapportages, melding bij AP | A | R | R | S | I | I |
| Melden van datalekken | A | R | R | C | S | C* |
| Transparante informatie | | | | | | |
| Privacy statement algemeen en Privacy statement medewerkers | A | R | R | S | I | I |
| Informatievoorziening op procesniveau | A | R | R | C | S | I |
| Beveiliging | | | | | | |
| Nemen van passende techniscen en organisatorische maatregelen | A | R | R | C** | S | I |
| Privacy by Design/Privacy by Default | | | | | | |
| Implementeren privacy by design en default in organisatie | A | R | R | S | C | I |
| Uitvoering geven aan privacy by design en by default principes | A | R | R | C | S | I |

* In afwijking van het Statuut Gegevensbescherming is in de Procedure Datalekken bepaald dat de privacy officer de melding van datalekken afhandeld en waar nodig de de functionaris Gegevensbescherming om advies vraagt

** In dit geval wordt de Information Security Officer geraadpleegd ipn de privacy officer