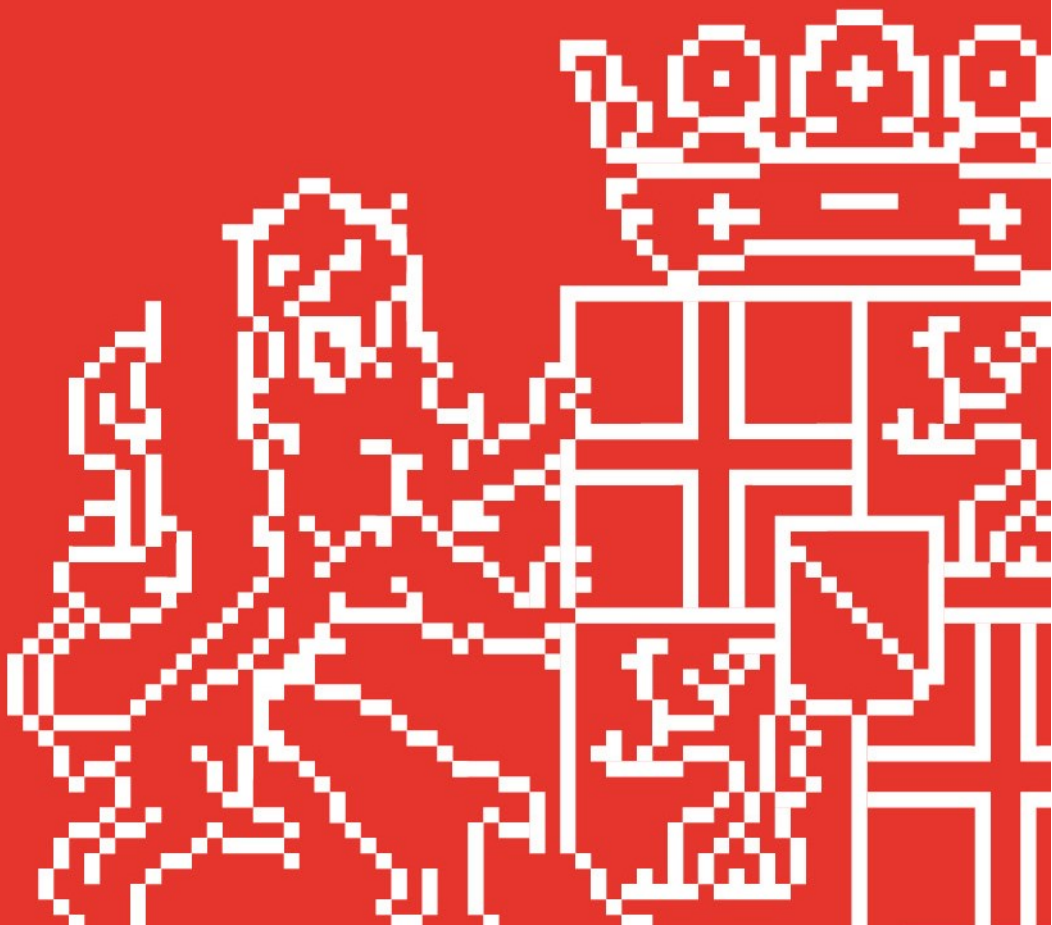
PROVINCIE UTRECHT

ALGEMEEN PRIVACYBELEID

PROVINCIE UTRECHT

2021-2025



PROVINCIE-UTRECHT.NL

Inhoudsopgave

1. Inleiding

1.1 Algemeen

Dit is het Algemeen Privacybeleid van de provincie Utrecht (Privacybeleid). Het doel van dit Privacybeleid is om op eenduidige en samenhangende wijze de uitgangspunten op het gebied van privacy te communiceren. De provincie Utrecht voert op uiteenlopende onderwerpen (bijvoorbeeld mobiliteit, cultuur en erfgoed, milieu en klimaat) wettelijke en bestuurlijke taken uit. 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. 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), acht de provincie Utrecht zich gehouden deze maatregelen vast te leggen in dit Privacybeleid.

Het Privacybeleid is vastgesteld door Gedeputeerde Staten en is geldig voor de periode van 2021-2025. In deze periode wordt dit Privacybeleid jaarlijks beoordeeld op actualiteit, juistheid en volledigheid en waar nodig bijgesteld. Aan het eind van deze periode – of eerder als interne of externe ontwikkelingen hiertoe noodzaken - zal Gedeputeerde Staten het Privacybeleid opnieuw vaststellen. De meest actuele versie van dit Privacybeleid is steeds terug te vinden op de website van de provincie Utrecht.

1.2 Visie en kernwaarden

De provincie Utrecht geeft veel aandacht aan en stopt veel inzet in het voldoen aan privacy wet- en regelgeving. Hierbij heeft de provincie de ambitie om te groeien naar een privacy volwassenheidsniveau CIP niveau 3 in 2025. 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.

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:

- 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.

1.4 Wetten en regels

Het Privacybeleid is in hoofdlijnen gebaseerd op de AVG[1]. In de AVG zijn de belangrijkste regels voor de rechtmatige omgang met Persoonsgegevens vastgelegd. Artikel 24 van de AVG regelt onder andere dat de Verwerkingsverantwoordelijke een passend Privacybeleid moet opstellen.

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 het Europees Comité voor Gegevensbescherming.[2] 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),[3] die van toepassing is op de provincie Utrecht, zijn normen bepaald voor informatieveiligheid. In het *Informatiebeveiligingsbeleid* wordt hier verder invulling aan gegeven.

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. Bij de naleving van deze andere wet- en regelgeving zal zorgvuldig worden gekeken hoe deze wetgeving zich verhoudt tot de verplichtingen van de AVG.

[1] Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG).
[2] 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.
[3] https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/.

1.5 Nadere uitwerking Privacybeleid

Dit Privacybeleid wordt op onderdelen verder uitgewerkt in nadere beleidsdocumenten, richtlijnen, werkinstructies en/of templates. Waar dit van toepassing is, wordt daar in dit Privacybeleid specifiek naar verwezen. Een overzicht hiervan zoals aanwezig ten tijde van het vaststellen van dit beleid is opgenomen in Bijlage 2.

1.6 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 te kunnen aantonen. Over de uitvoering van het privacybeleid legt Gedeputeerde Staten – mede op basis van de jaarrapportage van de FG – 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, de FG, de privacy officer en uiteindelijk iedere medewerker van de provincie Utrecht. Dit is verder uitgewerkt in het *Statuut Gegevensbescherming*.[4]

1.7 Controle, naleving en stimuleren

Bij de provincie Utrecht is concern control verantwoordelijk voor concern breed onderzoek en audit op het gebied van privacy (en informatiebeveiliging). De FG is verantwoordelijk voor het houden van toezicht op de inrichting en werking van de organisatie m.b.t. naleving van de AVG en rapporteert periodiek over de naleving van privacy wet- en regelgeving binnen de provincie Utrecht en over uitgevoerde onderzoeken.

Controle op naleving bestaat uit concreet toezicht op de dagelijkse praktijk van de privacy processen. Van belang hierbij is dat de medewerkers actief worden gestimuleerd in het juiste gedrag met betrekking tot naleving van de AVG.

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

2. Privacybeleid

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.

2.1 Bewustwording

De provincie Utrecht borgt dat alle medewerkers een hoog niveau van bewustwording hebben op het gebied van privacy. Informatieveiligheid en Privacy (hierna: IV&P) is een vast onderdeel van de introductiecursus voor nieuwe medewerkers, en deze kennis wordt actueel gehouden met onder andere e-learnings, voorlichtingscampagnes en gerichte presentaties aan management en medewerkers. Daar waar privacy medewerkers al deze bewustwordingsactiviteiten kunnen voorbereiden en uitvoeren, heeft het lijnmanagement een verantwoordelijkheid voor het blijvend onder de aandacht brengen van het belang van IV&P voor iedere medewerker, bijvoorbeeld via de jaarlijkse planning & control en voortgangsgesprekken.

2.2 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. De provincie Utrecht bewaart Persoonsgegevens in ieder geval in overeenstemming met selectielijsten voor archiefbescheiden van de Provinciale Organen. 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.

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 de wet voorschrijft om de desbetreffende Persoonsgegevens te bewaren, verwijdert de provincie deze gegevens pas als de wettelijke bewaartermijn verlopen is.

Nadere uitwerking van dit onderwerp is opgenomen in het '*Beleidsdocument bewaartermijn persoonsgegevens*', dat medewerkers van de provincie Utrecht tevens duidelijke kaders biedt voor het bepalen, vastleggen en borgen van de bewaartermijn van persoonsgegevens.

2.3 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

In het register van verwerkingsactiviteiten wordt per Verwerking vastgelegd welke Persoonsgegevens door de provincie worden verwerkt. Indien een Data Protection Impact Assessment (DPIA) heeft plaats gevonden, is daarin expliciet aandacht geschonken aan het onderwerp data-minimalisatie. Proceseigenaren zijn verantwoordelijk voor de juistheid van de Persoonsgegevens van hun processen zoals opgenomen in het Verwerkingsregister. Mochten Betrokkenen van mening zijn of vermoeden dat hun Persoonsgegevens niet juist zijn, kunnen zij een verzoek indienen deze te wijzigen, blokkeren of verwijderen. Dit is geregeld in de '*Procedure verzoeken rechten betrokkenen'*.

2.4 Delen met derden 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 heeft. Deze afspraken moeten ten minste voldoen aan de AVG, en kunnen worden vastgelegd in een Verwerkersovereenkomst, een onderlinge regeling of een gegevensleveringsovereenkomst.

In de *Werkinstructie Verwerkersovereenkomst* (en andere privacyovereenkomsten) is aan de hand van een beslisboom uitgewerkt of en, zo ja, welke privacyovereenkomst gesloten moet worden. Indien een verwerkersovereenkomst afgesloten moet worden, kan gebruik gemaakt worden van een door de provincie Utrecht opgestelde '*Model Verwerkersovereenkomst'* welke inhoudelijk voldoet aan de eisen die de AVG daaraan stelt. 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.

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.

Met betrekking tot doorgifte aan partijen in derde landen 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. Bepalen of een doorgifte van persoonsgegevens rechtmatig is, is nadere uitgewerkt in de '*Werkinstructie doorgifte persoonsgegevens*'.

2.5 Doelbinding

De 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 verenigbaar 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 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.

2.6 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 worden bewust gemaakt van de vertrouwelijkheid van Persoonsgegevens, onder andere door het afnemen van de eed/belofte en door het organiseren van diverse bewustwordingsactiviteiten (waaronder een e-learning IV&P);
- Er is een Informatiebeveiligingsbeleid;
- Er zijn regels ingevoerd omtrent de classificatie van (de vertrouwelijkheid van) documenten;
- Er zijn templates voor het uitvoeren van een Quickscan en/of een DPIA;
- Er is een Procedure Datalekken.

2.7 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 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

Betrokkenen worden over hun rechten geïnformeerd door middel van de algemene privacy verklaring op de website van de provincie Utrecht of door middel van afzonderlijke privacy

verklaringen voor specifieke verwerkingen. Intern heeft de provincie Utrecht een vastgestelde *Procedure rechten van betrokkenen*, waarin is beschreven op welke wijze verzoeken van Betrokkenen binnen de provincie Utrecht worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft. Deze procedure waarborgt een tijdige afhandeling van de verzoeken.

2.8 Rechtmatigheid

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 rechtmatigheid houdt in dat de provincie Utrecht alleen Persoonsgegevens verwerkt als hier een wettelijke grondslag voor is. Dit is verder uitgewerkt in '*Richtlijn IBP8 – Wettelijke Grondslag*'. De wettelijke grondslag van de Verwerking wordt opgenomen in het Verwerkingsregister.

2.9 Verwerkingsregister

Om invulling te kunnen geven aan de verplichtingen die voortvloeien uit het verwerken van Persoonsgegevens, heeft de provincie Utrecht een register van de verwerkingsactiviteiten (Verwerkingsregister) opgesteld, zoals genoemd in artikel 30 van de AVG. In dit Verwerkingsregister worden de belangrijkste aspecten van de Verwerking opgenomen, zoals doel, wettelijke grondslag, aard van de Persoonsgegevens, op wie ze betrekking hebben, wie er toegang tot hebben, de bewaartermijn, en welke maatregelen er zijn genomen om deze Persoonsgegevens te beschermen.

In het '*Beleidsdocument verwerkingsregister*' zijn de rollen en verantwoordelijkheden ten aanzien van het beheer van het Verwerkingsregister vastgelegd. Proceseigenaren zijn verantwoordelijk voor de inhoud, compleetheid en actualiteit van de opgenomen Verwerkingen. De Privacy Officers voeren het functioneel beheer over het Verwerkingsregister en adviseren de proceseigenaren; hierbij hebben zij ook een 'aanjaagrol' jegens de provincie en de proceseigenaren in het bijzonder. De FG houdt toezicht op dit geheel. Via intranet is het verwerkingsregister in te zien door alle medewerkers van de PU. Alleen de privacy officers kunnen (al dan niet op instigatie van de proceseigenaar) wijzigingen doorvoeren.

2.10 Data Protection Impact Assessment (DPIA)

Voor de provincie Utrecht geldt dat voor een nieuwe Verwerking of een wijziging in een bestaande Verwerking een Quickscan uitgevoerd dient te worden. Een Quickscan wordt door een Information Security Officer en een Privacy Officer samen met de proceseigenaar uitgevoerd. Hiervoor is een Quickscan template ontwikkeld. Aan de hand van de uitgevoerde Quickscan wordt voor informatiebeveiliging een risicoanalyse uitgevoerd als er aanleiding toe is. Op basis van de uitgevoerde Quickscan wordt tevens bepaald of voor een afzonderlijke Verwerking een hoog risico bestaat en een DPIA noodzakelijk is.

Indien er sprake is van Verwerkingen met een hoog privacy risico voor Betrokkenen, dient er conform artikel 35 van de AVG voorafgaand aan die verwerking een DPIA uitgevoerd te worden. 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 *DPIA Template* voor de uitvoering van een DPIA. Proceseigenaren zijn verantwoordelijk voor de uitvoering van een DPIA voor een Verwerking met een hoog privacy risico. Privacy Officers en Information Security Officers ondersteunen en adviseren bij de uitvoering hiervan. De FG geeft advies over de uitgevoerde DPIA (artikel 35 lid 2 AVG) en ondertekent de DPIA. De Privacy Officers houden een overzicht bij van de uitgevoerde DPIA´s en monitoren de voortgang van te implementeren beheersmaatregelen.

Processen kunnen regelmatig worden aangepast. Dit kan ook effect hebben op de Verwerking van Persoonsgegevens. Als er een wijziging in het proces wordt doorgevoerd, kan het noodzakelijk zijn 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. In beginsel dient een DPIA na drie jaar te worden geactualiseerd. 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 kunnen adviseren over de eventuele verkorting van de periodiciteit.

2.11 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. 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 2.10 geldt voor de provincie Utrecht dat voor een nieuwe Verwerking of een wijziging in een bestaande Verwerking een Quickscan uitgevoerd dient te worden. Bij het uitvoeren van een Quickscan, 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. Ook zijn er vanuit *privacy inkoopeisen* opgesteld die meegenomen dienen te worden bij aanbestedingen voor systemen waar persoonsgegevens in verwerkt kunnen worden.

2.12 Datalekken

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

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 onverwijld, 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, dient er een motivering voor de vertraging bij de melding te worden gevoegd. Indien het

Datalek een hoog risico met zich meebrengt voor Betrokkenen, meldt de provincie Utrecht dit ook aan de Betrokkenen zelf.

De provincie Utrecht heeft een vastgestelde *Procedure Datalekken* 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. Deze procedure is tezamen met verdere uitleg via Intranet beschikbaar voor medewerkers. Daarnaast is het melden van Datalekken een terugkerend onderwerp bij awareness activiteiten.

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

2.13 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. De FG is er niet verantwoordelijk voor of zijn adviezen wel of niet worden uitgevoerd. Wel moeten de FG en het bestuur van de organisatie samen vastleggen wat er met de adviezen van de FG gebeurt. En waarom bepaalde adviezen eventueel niet zijn overgenomen (‘comply or explain’). De FG heeft een aanjagende functie en stimuleert de organisatie om zich bewust te worden van de privacyrisico’s.

De FG maakt jaarlijks een FG toezichtplan. De FG draagt zorg voor periodieke rapportage over de naleving van privacy wet- en regelgeving binnen de provincie Utrecht. De FG rapporteert een keer per jaar in een jaarverslag en een keer per jaar in een tussentijds verslag, en rapporteert tevens over uitgevoerde onderzoeken.

De FG heeft onder meer de volgende wettelijke taken:

- Informeren en adviseren van de organisatie over de verplichtingen uit hoofde van de privacy wet- en regelgeving;
- 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;
- Adviseren bij en toezien op de uitvoering van DPIA’s en bij beoordeling van Datalekken.

2.14 Beveiliging

Op grond van de AVG dienen organisaties passende technische en organisatorische maatregelen te nemen om de Persoonsgegevens die zij verwerken, te beveiligen. De provincie Utrecht heeft een Informatiebeveiligingsbeleid opgesteld waarin is beschreven op welke wijze invulling is gegeven aan

de passende beveiliging van Persoonsgegevens. Tevens zijn er een Corporate Information Security Officer (hierna: CISO) een Technical Information Security Officer (hierna: TISO) en Information Security Officers aangesteld.

2.15 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* op haar website waarin Betrokkenen worden geïnformeerd over de Verwerking van Persoonsgegevens door de provincie Utrecht. Sollicitanten bij de provincie Utrecht en Medewerkers van de provincie Utrecht zijn ook Betrokkenen. Voor beide doelgroepen zijn een afzonderlijke Privacy Verklaringen opgesteld die bij de sollicitatie dan wel de indiensttreding actief wordt aangeboden. Aanvullend hierop worden alle Betrokkenen bij specifieke processen, waar mogelijk en noodzakelijk, aanvullend geïnformeerd over de betreffende gegevensverwerking.

De provincie Utrecht draagt zorg dat, indien hier om wordt verzocht (zie paragraaf 2.7 inzake de rechten van betrokkenen), de Betrokkene de voor het verzoek relevante informatie krijgt omtrent de verwerkte Persoonsgegevens.

2.16 Risicomanagement

De provincie Utrecht baseert zich voor compliance en volwassenheid ten aanzien van de AVG op de Privacy baseline en het Privacy volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacybescherming (CIP). Middels het uitvoeren van periodieke assessments op basis van dit normenkader en het analyseren van de resultaten van deze assessments, worden strategische en tactische privacy risico's in kaart gebracht en worden maatregelen genomen om deze risico's te beheersen zodat grip op privacy gewaarborgd blijft.

Daarnaast worden risico's in kaart gebracht voor Verwerkingen van persoonsgegevens waarbij sprake is van een verhoogd privacy risico voor Betrokkenen. Deze risico's worden in kaart gebracht door voorafgaand aan de verwerkingen een Data Protection Impact Assessment (DPIA) uit te voeren. Een DPIA geeft inzicht in de privacy risico's en welke maatregelen getroffen moeten worden om deze risico beheersbaar te maken.

Bijlage 1 IV&P Beleidsdocumenten, richtlijnen, werkinstructies en templates

Onderstaande documenten zijn voor alle medewerkers beschikbaar via de intranetpagina van IV&P

Beleidsdocumenten

Procedure verzoeken rechten betrokkenen

Privacy Statement (intern en extern)

Informatiebeveiligingsbeleid

Beleidsdocument Verwerkingsregister

Beleidsdocument bewaartermijn persoonsgegevens

Protocol controle en onderzoek bedrijfsmiddelen

Procedure Datalekken

Richtlijnen en werkinstructies

Anonimiseren bij publicatie

BSN-nummers en kopieën van identiteitsbewijzen

Fotograferen en filmen

Organiseren bijeenkomsten en webinars

Regels en classificatie omtrent documenten

Wachtwoord

Wettelijke grondslag

Werkinstructie doorgifte persoonsgegevens

Werkinstructie DPIA's

Werkinstructie Verwerkersovereenkomst (en andere privacyovereenkomsten)

Inkoopeisen privacy

Templates

Privacy-overeenkomsten:

- Model verwerkersovereenkomst PU
- Addendum bij bestel- en bezorgovereenkomsten
- Model gegevensleveringsovereenkomst
- Model samenwerkingsprotocol AVG

Quickscan Template

DPIA Template

Meldingsformulier datalekken

Registers

Verwerkingsregister

Datalekregister

Register verzoeken betrokkenen

Bijlage 2 Definities

In dit 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[5] zijn blootgesteld aan onrechtmatige toegang/verstrekking, diefstal, verlies, vernietiging enzovoort.[6]

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

[5] 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.
[6] 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.

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.

Verwerkingsregister

Het register van de verwerkingsactiviteiten zoals genoemd in artikel 30 van de AVG.

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).