provincie Gelderland

PRIVACYBELEID PROVINCIE GELDERLAND

Colofon			
Eigenaar	: Provincie Gelderland		
Titel	:	Privacybeleid	
Status document	:	V 1.2	
Auteur(s)	:	5.1.2e (naar voorbeeld van Prov. Utrecht)	
Versiebeheer			
Versie	Datum	Auteur(s)	Wijziging
0.1			
0.2	5-1-2023	5.1.2e	Gehele document gereviewed, aangepast voor PG en links naar bestaande documenten toegevoegd
0.8			Verwerken opmerkingen en klaar maken voor PO-overleg
0.9	23-3-2023		Concept gereed voor behandeling in Stuurgroep Privacy. Stuurgroep heeft commentaar gegeven
1.0	06-06-2023		Commentaar van stuurgroep is verwerkt. Versie gereed om ter goedkeuring aan te bieden aan de directie/CMT.
1.0	19-06-2023		Vastgesteld door directie/CMT
1.1	22-10-2024		Kleine aanpassingen en actueel gemaakt.
1.2	13-10-2025		Actueel gemaakt en afgestemd op de huidige privacy organisatie, zoals goedgekeurd door de OR en directie).

Inhoud

1. Inleiding

1.1 Algemeen

Binnen de provincie Gelderland werken we dagelijks met persoonsgegevens van inwoners, medewerkers en partners. Deze gegevens hebben we nodig om onze wettelijke en autonome taken goed uit te voeren en om te zorgen voor een betrouwbare en goed functionerende organisatie.

Tegelijkertijd veranderen de eisen aan privacy en gegevensbescherming door technologische ontwikkelingen en digitalisering. Wij zijn ons daarvan bewust en nemen passende maatregelen om de privacy te waarborgen, zoals sterke informatiebeveiliging, dataminimalisatie en transparantie in wat we doen.

Inwoners en medewerkers moeten erop kunnen vertrouwen dat provincie Gelderland zorgvuldig en veilig met hun persoonsgegevens omgaat.

Met dit beleid geven wij richting aan hoe de provincie privacy waarborgt, beschermt en handhaaft. Het beleid geldt voor de gehele organisatie en voor alle processen en gegevensverzamelingen waarin persoonsgegevens voorkomen.

Het beleid bestaat uit twee delen:
- het algemene deel, waarin de uitgangspunten en verantwoordelijkheden zijn beschreven;
- de bijlagen, waarin de praktische werkwijzen en hulpmiddelen staan uitgewerkt.

Dit privacybeleid is vastgesteld door het directieteam (CMT), na instemming van de Ondernemingsraad (OR). Als interne of externe ontwikkelingen daartoe aanleiding geven, kan het tussentijds worden aangepast. Bij significante wijzigingen met gevolgen voor betrokkenen wordt het opnieuw vastgesteld.

1.2 Wetten en regels

Dit privacybeleid is gebaseerd op zowel Europese als nationale wetgeving, met name de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG). De AVG bevat de algemene regels voor een rechtmatige verwerking van persoonsgegevens; de UAVG werkt de nationale keuzes voor Nederland verder uit.

De AVG verplicht verwerkingsverantwoordelijken om een passend privacybeleid op te stellen. Bij de uitvoering daarvan volgt de provincie Gelderland de beleidsregels, richtsnoeren en opinies van de Autoriteit Persoonsgegevens en het Europees Comité voor Gegevensbescherming (EDPB).

Bescherming van persoonsgegevens is onlosmakelijk verbonden met informatieveiligheid. Informatieveiligheid vormt een randvoorwaarde voor een zorgvuldige omgang met persoonsgegevens. De normen daarvoor zijn vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO), die van toepassing is op de provincie Gelderland.

Naast de AVG en de UAVG moet de provincie ook voldoen aan andere wet- en regelgeving die de verwerking van persoonsgegevens raakt of aanvullende verplichtingen oplegt. Waar sectorspecifieke wetgeving relevant is, wordt deze in het beleid of de bijlagen vermeld.

1.3 Definities

In het privacybeleid worden de volgende definities gehanteerd:

Algemene verordening gegevensbescherming (AVG)
Europese wet (Verordening EU 2016/679) die regels geeft voor het beschermen van persoonsgegevens en het vrije verkeer daarvan binnen de EU.

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

Rechten van betrokkenen
Op grond van de AVG heeft iedere betrokkene verschillende rechten, zoals het recht op inzage, rectificatie en aanvulling, verwijdering (het recht om vergeten te worden), dataportabiliteit, beperking van de verwerking, bezwaar, duidelijke informatie en het recht met betrekking tot geautomatiseerde besluitvorming en profilering.

Datalek
We spreken van een datalek indien vertrouwelijke informatie van provincie Gelderland en/of persoonsgegevens zijn blootgesteld aan onrechtmatige toegang/verstrekking, diefstal, verlies, vernietiging enzovoort.

Data Protection Impact Assessment (DPIA)
Een DPIA is een hulpmiddel om vooraf de privacyrisico's van een verwerking in beeld te brengen. Zo kunnen we maatregelen nemen om die risico's te verkleinen. Een DPIA is verplicht als een verwerking waarschijnlijk een hoog risico oplevert voor de privacy van betrokkenen. Bij provincie Gelderland doen we eerst een pre-DPIA om te bepalen of een volledige DPIA nodig is.

Functionaris Gegevensbescherming (FG)
De FG is een onafhankelijke toezichthouder binnen de provincie. Hij of zij controleert of de provincie zich houdt aan de privacywetgeving en adviseert over verbeteringen.

Centrale Privacy Officers (CPO's)
De Centrale Privacy Officers vormen het privacyteam van de provincie Gelderland. Zij adviseren afdelingen over de toepassing van de AVG, helpen bij het uitvoeren van (pre)DPIA's en verwerkersovereenkomsten, geven cursussen en zorgen voor een goede afstemming met de FG.

Verder houden zij toezicht op de naleving van het privacybeleid, bewaken de voorgang van acties en helpen (zo nodig) de privacy ambassadeurs in de uitvoering.

Chief Privacy Officer
De Chief Privacy Officer, onderdeel van het centrale privacyteam) bewaakt het privacybeleid en de naleving van de AVG op strategisch niveau.

Privacy Ambassadeur
Elke afdeling heeft één of meer privacy ambassadeurs. Zij zijn het eerste aanspreekpunt binnen hun afdeling voor vragen of signalen over privacy. De privacy-ambassadeur helpt collega's om zorgvuldig met persoonsgegevens om te gaan, signaleert risico's en bespreekt deze met de centrale privacy officer(s). Indien nodig wordt de FG betrokken.

CISO (Chief Information Security Officer)
De CISO is verantwoordelijk is voor het implementeren van informatiebeveiligingsbeleid én het toezicht daarop. Dit heeft een nauwe relatie met privacy.

Autoriteit Persoonsgegevens (AP)
De Autoriteit Persoonsgegevens houdt zich binnen Nederland bezig met het toezicht op de naleving van de AVG en UAVG.

Persoonsgegevens
Alle gegevens die gaan over natuurlijke (levende) personen en waaraan je iemand als individu kunt herkennen, zijn persoonsgegevens. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat is te herleiden tot een persoon (bijvoorbeeld: naam, adres, geboortedatum, locatie of BSN).

Naast gewone persoonsgegevens kent de AVG ook bijzondere persoonsgegevens. Dit zijn gegevens die door hun aard extra gevoelig zijn, zoals etnische afkomst, gezondheid, politieke opvattingen of genetische en biometrische gegevens. De verwerking van bijzondere persoonsgegevens is verboden, tenzij een wettelijke uitzondering van toepassing is. In dat geval moet er bovendien altijd een geldige grondslag voor de verwerking zijn.

Verwerker
Een organisatie of persoon die namens de provincie persoonsgegevens verwerkt. De verwerker doet dit volgens de afspraken met de provincie en mag de gegevens niet voor eigen doelen gebruiken.

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

Verwerkingsverantwoordelijke
De organisatie of persoon die bepaalt waarom (het doel) en de essentiële middelen waarmee persoonsgegevens worden verwerkt. Essentiële middelen zijn de belangrijkste keuzes over hoe dat gebeurt. Denk aan welke gegevens worden verzameld, waarom ze nodig zijn, wie ze mag gebruiken, hoe lang ze worden bewaard en of ze worden gedeeld met anderen. De verwerkingsverantwoordelijke kan dit alleen of samen met een andere partij vaststellen.

Verwerkersovereenkomst
Een schriftelijke overeenkomst tussen de provincie en een verwerker. Daarin staat hoe de verwerker met persoonsgegevens moet omgaan, welke beveiligingsmaatregelen gelden en dat de gegevens alleen in opdracht van en namens de provincie mogen worden gebruikt.

Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)
De UAVG is de Nederlandse wet die uitlegt hoe de regels van de AVG in Nederland gelden.
De UAVG vult de AVG aan en regelt bijvoorbeeld welke uitzonderingen of keuzes in Nederland van toepassing zijn.

Verwerkingsregister
De provincie houdt een verwerkingsregister bij. Dat is een overzicht van alle verwerkingen van persoonsgegevens binnen de organisatie. In het register staat onder andere:
welke gegevens we verwerken, voor welk doel, op basis van welke grondslag, wie de gegevens gebruikt, en hoe lang ze worden bewaard. Dit register helpt om te controleren of we voldoen aan de AVG.

Dataminimalisatie
De AVG zegt dat we zo weinig mogelijk persoonsgegevens mogen verwerken. We gebruiken dus alleen de gegevens die echt nodig zijn voor het doel. Iedere medewerker moet bij het verwerken van gegevens nagaan of elk gevraagd gegeven nodig is.

Privacyverklaring
De privacyverklaring legt uit hoe de provincie omgaat met persoonsgegevens. Daarin staat welke gegevens we verzamelen, waarom we dat doen en welke rechten mensen hebben.
Er zijn twee privacyverklaringen:

- één voor inwoners, bedrijven en andere externe partijen (te vinden onderaan de website van de provincie);
- en één voor medewerkers, waarin staat hoe de provincie omgaat met personeelsgegevens (beschikbaar op het plein en op de Sharepointpagina 'Privacy & AVG").

1.4 Visie en kernwaarde

Provincie Gelderland wil dat iedereen kan vertrouwen op een veilige verwerking van persoonsgegevens. Vertrouwen in onze dienstverlening is daarbij essentieel. Onze ambitie is om privacy continu verder te versterken.

1.5 Reikwijdte en afbakening privacy

Dit privacybeleid geldt voor de hele organisatie van provincie Gelderland: voor alle processen, onderdelen en gegevensverzamelingen waarin persoonsgegevens voorkomen.
Het beleid heeft betrekking op alle verwerkingen waarbij de provincie zelfstandig of samen met anderen verwerkingsverantwoordelijke is. Het omvat de volledige levenscyclus van gegevens – van verzamelen en gebruiken tot opslaan, archiveren en verwijderen.

Dit beleid is bedoeld voor intern gebruik. Derden kunnen het op verzoek inzien. Voor extern gebruik is er een aparte privacyverklaring beschikbaar op gelderland.nl.

1.6 Nadere uitwerking privacybeleid

Bij bepaalde organisatieonderdelen stelt provincie Gelderland, in aanvulling op het algemene privacybeleid, specifiek uitvoeringsbeleid, nadere richtlijnen of werkwijzen op. Waar dit van toepassing is, wordt in dit privacybeleid naar die specifieke beleidsregels verwezen. Dit geldt ook voor werkterreinen waar – naast de AVG – andere wetten zoals de Wet politiegegevens (Wpg) gelden.

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 provincie Gelderland 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 provincie Gelderland zorgt dat er transparant wordt gecommuniceerd over het gebruik van persoonsgegevens.

2.2 Privacy uitgangspunten

Provincie Gelderland hanteert de volgende privacy uitgangspunten die in de volgende paragrafen worden beschreven.

2.2.1 Bewaren van persoonsgegevens

Provincie Gelderland bewaart persoonsgegevens niet langer dan nodig is voor het doel waarvoor ze zijn verzameld. Als een wettelijke bewaartermijn geldt, houden wij die aan.

Gegevens worden verwerkt op basis van een taak van algemeen belang of een wettelijke verplichting. Voor personeelsgegevens geldt daarnaast dat verwerking plaatsvindt in het kader van de arbeidsovereenkomst. Na het verlopen van de bewaartermijn verwijdert of anonimiseert de provincie de persoonsgegevens.

Bij een verzoek om gegevens te verwijderen beoordeelt de provincie eerst of dit wettelijk is toegestaan en of er specifieke afspraken gelden over bewaartermijnen, zoals de interprovinciale selectielijst van het Nationaal Archief.

2.2.2 Dataminimalisatie en juistheid

Provincie Gelderland verwerkt alleen de persoonsgegevens die echt nodig zijn voor het doel. We zorgen er ook voor dat deze gegevens juist en actueel blijven.

2.2.3 Delen met derden

Als provincie Gelderland persoonsgegevens deelt met andere partijen, maken we hierover duidelijke afspraken. Deze afspraken voldoen aan de AVG en worden vastgelegd in een overeenkomst, zoals een verwerkersovereenkomst of een onderlinge regeling.

Er is een **Model verwerkersovereenkomst** aanwezig dat inhoudelijk voldoet aan de eisen die de AVG daaraan stelt. Provincie Gelderland houdt de verwerkers waarmee een verwerkersovereenkomst is afgesloten bij in het verwerkingsregister. De ondertekende versies van de verwerkersovereenkomsten worden gearchiveerd.

2.2.4 Doelbinding

Provincie Gelderland verzamelt alleen persoonsgegevens voor duidelijke en gerechtvaardigde doelen (zie ook paragraaf 2.2.7). Bij het gebruik van persoonsgegevens letten we op proportionaliteit en subsidiariteit. Dat betekent dat we alleen gegevens verwerken die echt nodig zijn voor het doel en dat we altijd kiezen voor de minst ingrijpende manier. Persoonsgegevens worden alleen voor een ander doel gebruikt als dat nieuwe doel goed past bij het oorspronkelijke doel waarvoor de gegevens zijn verzameld.

2.2.5 Integriteit en vertrouwelijkheid

Provincie Gelderland gaat zorgvuldig om met de haar toevertrouwde persoonsgegevens. Provincie Gelderland neemt passende beveiligingsmaatregelen om persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, verlies of wijziging, ongeautoriseerde openbaarmaking, misbruik of anderszins verwerking in strijd met de wet.

2.2.6 Rechten van Betrokkenen

De AVG bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel 'de rechten van betrokkenen' genoemd, en bestaan uit:

- **Recht op inzage**: Het recht van betrokkenen om onder meer een kopie te ontvangen van de persoonsgegevens die u van hen verwerkt.
- **Recht op vergetelheid**: Betrokkenen hebben het recht om 'vergeten' te worden.
- **Recht op rectificatie en aanvulling**: Betrokkenen hebben het recht om persoonsgegevens die worden verwerkt te laten wijzigen.
- **Recht op dataportabiliteit:** Betrokkenen hebben het recht om persoonsgegevens over te (laten) dragen aan een andere partij.
- **Recht op beperking van de verwerking**: Het recht om minder gegevens te laten verwerken.
- **Het recht met betrekking tot geautomatiseerde besluitvorming en profilering.** Oftewel: betrokkenen hebben het recht op een menselijke blik bij besluiten.
- **Recht op bezwaar**: Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens.
- **Recht op duidelijke informatie:** Betrokkenen hebben recht op duidelijke informatie over wat er met hun gegevens gebeurt.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Derden via de website van provincie gelderland en medewerkers via het Plein (intranet). Provincie Gelderland 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. Tevens zorgen we ervoor dat de betrokkenen binnen de wettelijk gestelde reactietermijn een reactie ontvangt.

Provincie Gelderland heeft een vastgestelde **Procedure rechten van betrokkenen** waarin is beschreven op welke wijze verzoeken van betrokkenen binnen provincie Gelderland worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft.

2.2.7 Rechtmatigheid en transparantie

Provincie Gelderland verwerkt persoonsgegevens altijd op een rechtmatige, zorgvuldige en transparante manier, volgens de AVG en andere wetgeving. We verwerken alleen gegevens als daar een geldige grondslag voor is. De AVG noemt zes grondslagen voor het verwerken van persoonsgegevens:

- Toestemming: de persoon heeft daarvoor toestemming gegeven.
- Overeenkomst: de verwerking is nodig om een overeenkomst uit te voeren (bijvoorbeeld een arbeidsovereenkomst).
- Wettelijke verplichting: de verwerking is verplicht op grond van de wet.
- Vitale belangen: de verwerking is nodig om iemands leven of gezondheid te beschermen.
- Taak van algemeen belang of openbaar gezag: de verwerking is nodig om een publieke taak uit te voeren.
- Gerechtvaardigd belang: de verwerking is nodig voor een eigen belang van de organisatie, maar alleen als dit belang zwaarder weegt dan de privacy van de betrokkene.

Voor de provincie geldt dat:

- verwerkingen voor inwoners en bedrijven vindt in beginsel plaats op basis van een taak van algemeen belang of openbaar gezag, en
- verwerkingen als werkgever vindt in beginsel plaats op basis van wettelijke verplichtingen of de arbeidsovereenkomst.

Elke grondslag heeft zijn eigen voorwaarden en beperkingen; deze worden per verwerking beoordeeld.

Provincie Gelderland heeft procedures en protocollen opgesteld om te waarborgen dat haar medewerkers weten hoe zij om moeten gaan met persoonsgegevens. Alle medewerkers worden (bij)geschoold om op de hoogte te raken over hun AVG-verantwoordelijkheden.

Provincie Gelderland draagt zorg dat, indien hierom 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.

2.2.8 Geautomatiseerde verwerkingen

Als persoonsgegevens automatisch worden gebruikt om iets over een persoon te zeggen of te voorspellen, noemen we dat profilering. Daarbij wordt gekeken naar persoonlijke kenmerken, zoals iemands financiële situatie, interesses, gedrag of locatie.

Provincie Gelderland doet niet aan profilering.

2.3 Verplichtingen AVG

2.3.1 Register van verwerkingsactiviteiten

Om te voldoen aan de verplichtingen uit de AVG houdt provincie Gelderland een verwerkingsregister bij (artikel 30 AVG). In dit register staat onder andere:

- de naam en contactgegevens van de provincie en de Functionaris Gegevensbescherming (FG);
- de doelen van de verwerkingen;
- de categorieën persoonsgegevens en betrokkenen;
- met wie de gegevens worden gedeeld (ontvangers of gezamenlijke verwerkingsverantwoordelijken);
- eventuele doorgiften buiten de EER;
- de bewaartermijnen en een algemene beschrijving van de beveiligingsmaatregelen.

Het verwerkingsregister wordt beheerd in Trustbound, de privacy-applicatie van de provincie.

De proceseigenaren zijn verantwoordelijk voor het aanleveren en actualiseren van hun verwerkingen. De centrale privacy officers adviseren hierbij en controleren de kwaliteit van de invoer. De FG houdt toezicht op het geheel.

Twee keer per jaar vragen de privacy officers de proceseigenaren om hun gegevens te controleren en waar nodig te actualiseren. De taken en verantwoordelijkheden zijn uitgewerkt in de bijlagen bij dit beleid. Om invulling te kunnen geven aan de verplichtingen die voortvloeien uit het verwerken van persoonsgegevens, heeft provincie Gelderland een verwerkingsregister opgesteld, zoals genoemd in artikel 30 AVG.

2.3.2 Data Protection Impact Assessment

Een DPIA (Data Protection Impact Assessment) helpt om privacyrisico's in kaart te brengen en

maatregelen te nemen zodat deze risico's zo klein mogelijk blijven. De pre-DPIA en, als dat nodig is, de volledige DPIA worden (in de hoofdregel) uitgevoerd voordat een nieuwe verwerking start.

Bij provincie Gelderland geldt dat voor elke nieuwe verwerking of een grote wijziging in een bestaande verwerking wordt bekeken of een DPIA nodig is. Dit gebeurt met behulp van de pre-DPIA.
De (pre-)DPIA wordt ingevuld door de projectleider, opdrachtgever of proceseigenaar en daarna besproken met de centrale privacy officer. De Functionaris Gegevensbescherming (FG) geeft advies over de DPIA en ondertekent het document. Als het advies van de FG niet, of niet volledig, wordt overgenomen, moet duidelijk worden uitgelegd waarom.

Er zijn over dit onderwerp diverse procedures en template in de bijlagen aanwezig, opgenomen in Trustbound.

2.3.3 Privacy by Design en Privacy by Default

Volgens artikel 25 AVG moeten bij elke verwerking van persoonsgegevens Privacy by Design en Privacy by Default worden toegepast.

Privacy by Design betekent dat al tijdens het ontwerpen van processen, systemen of diensten wordt nagedacht over de bescherming van persoonsgegevens. Er wordt vooraf gekeken welke technische en organisatorische maatregelen nodig zijn om gegevens goed te beveiligen. Een belangrijk uitgangspunt daarbij is dataminimalisatie: alleen gegevens verwerken die echt nodig zijn. In het Informatie-beveiligingsbeleid is vastgelegd dat privacy al aan het begin van projecten wordt meegenomen.

Privacy by Default houdt in dat systemen en programma's standaard zijn ingesteld op de meest privacyvriendelijke manier. Bij nieuwe of aangepaste verwerkingen voert provincie Gelderland een Business Impact Assessment (BIA) uit, zoals beschreven in het Informatiebeveiligingsbeleid.
Tijdens de BIA – en zo nodig een aanvullende DPIA – wordt beoordeeld of de verwerking voldoet aan de principes van Privacy by Design en Privacy by Default. Daarbij wordt onder andere gekeken naar dataminimalisatie en bewaartermijnen.

Op deze manier borgt de provincie dat nieuwe verwerkingen vanaf het begin zorgvuldig en privacyvriendelijk zijn ingericht.

2.3.4 Datalekken

Er is sprake van een datalek als informatie van provincie Gelderland of persoonsgegevens terechtkomt bij iemand die daar geen recht op heeft, of als deze gegevens verloren, gestolen of vernietigd zijn.

Wanneer een datalek heeft plaatsgevonden en dit waarschijnlijk een risico vormt voor de rechten en vrijheden van betrokkenen, moet het worden gemeld aan de Autoriteit Persoonsgegevens (AP).
De Functionaris Gegevensbescherming (FG) doet deze melding zo snel mogelijk, maar uiterlijk binnen 72 uur nadat het datalek bekend is geworden.
Als de melding later wordt gedaan, wordt uitgelegd waarom dat is. Wanneer het datalek een hoog risico oplevert voor betrokkenen, informeert de provincie ook de betrokkenen zelf.

Provincie Gelderland heeft een Procedure Datalekken waarin precies staat hoe datalekken worden afgehandeld en wie welke taken en verantwoordelijkheden heeft. Hierin staat ook beschreven wanneer en op welke manier de AP en/of de betrokkenen worden geïnformeerd.

Medewerkers kunnen informatie over het melden van datalekken vinden op het Serviceplein, onder het onderwerp “Melding vermoeden datalek”. Het melden van datalekken is dan ook een vast onderdeel van de privacy awareness-activiteiten.

Ook derden (zoals burgers, bedrijven of leveranciers) kunnen een mogelijk datalek melden.
Dit kan via het algemene contactformulier op de website van provincie Gelderland of per e-mail naar privacy@gelderland.nl. De melding komt dan terecht bij het privacyteam, dat beoordeelt of er sprake is van een datalek en welke vervolgstappen nodig zijn.

Alle datalekken en beveiligingsincidenten worden vastgelegd in Trustbound, het interne register van de provincie. Daarin staat of een incident heeft geleid tot een datalek en, zo ja, of dit is gemeld aan de AP en/of de betrokkenen. Elke melding wordt geëvalueerd, zodat herhaling in de toekomst kan worden voorkomen.

2.3.5 Functionaris gegevensbescherming (FG)

Provincie Gelderland is wettelijk verplicht een Functionaris Gegevensbescherming (FG) aan te stellen. De FG houdt toezicht op de naleving van de AVG en geeft gevraagd en ongevraagd advies over privacy. De contactgegevens staan op de website van de provincie.

De FG is onafhankelijk en wordt tijdig betrokken bij onderwerpen die met privacy te maken hebben. Als de provincie het advies van de FG niet volgt, wordt dit gemotiveerd aan hem of haar teruggekoppeld. Bij onrechtmatigheden of een zwaarwegend advies, bijvoorbeeld bij een DPIA, kan de FG het onderwerp escaleren naar de directie, GS of de Autoriteit Persoonsgegevens. De directie besluit uiteindelijk wat met het advies wordt gedaan.

De FG stelt jaarlijks een toezichtplan op en rapporteert over de uitvoering daarvan in een jaarverslag aan de directie.
Belangrijke taken van de FG zijn:

- adviseren en informeren over de AVG;
- toezicht houden op de uitvoering van privacybeleid, het verwerkingsregister en DPIA’s;
- beoordelen van datalekken;
- contact onderhouden met de Autoriteit Persoonsgegevens en de ondernemingsraad.

De provincie zorgt dat de FG zijn taken onafhankelijk kan uitvoeren en voldoende tijd, middelen en toegang heeft tot de benodigde informatie.

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. Provincie Gelderland heeft een **Informatiebeveiligingsbeleid** opgesteld waarin is beschreven op welke wijze invulling is gegeven aan de passende beveiliging van persoonsgegevens. Tevens is er een Chief Information Security Officer (CISO) aangesteld.

2.3.7. Transparante informatie

De AVG schrijft voor dat persoonsgegevens op een duidelijke en transparante manier moeten worden verwerkt. Mensen moeten weten welke gegevens van hen worden verzameld en waarvoor

die worden gebruikt.

Provincie Gelderland informeert betrokkenen hierover bij het verzamelen van hun gegevens.
Op de website van de provincie staat een privacyverklaring waarin wordt uitgelegd hoe persoonsgegevens worden verwerkt.
Daarnaast worden betrokkenen, waar dat nodig is, extra geïnformeerd bij specifieke processen of projecten.

2.3.8. Verwerkersovereenkomsten en doorgiften

Als provincie Gelderland de verwerking van persoonsgegevens uitbesteedt aan een andere partij (de verwerker), worden hierover duidelijke afspraken gemaakt. In deze afspraken staat hoe de verwerker met de gegevens mag omgaan en welke verplichtingen gelden. Deze afspraken worden vastgelegd in een verwerkersovereenkomst. Provincie Gelderland gebruikt hiervoor een eigen modelverwerkersovereenkomst dat voldoet aan de eisen van de AVG. In overleg kan ook een ander model worden gebruikt, als dit voldoet aan dezelfde eisen. De centrale privacy officers en de privacyjurist beoordelen of dat het geval is.

Soms is de provincie samen met een andere partij gezamenlijk verwerkingsverantwoordelijke. Dan wordt een onderlinge regeling gesloten waarin staat wie waarvoor verantwoordelijk is. Als er geen gezamenlijke verantwoordelijkheid is, kunnen de privacy officers en de FG adviseren om de afspraken vast te leggen in een verwerkersovereenkomst, samenwerkingsovereenkomst of gegevensleveringsdocument.

Voor doorgifte van persoonsgegevens geldt dat de provincie deze (hoofdregel) niet doorgeeft aan landen buiten de Europese Economische Ruimte (EER), tenzij dat aantoonbaar rechtmatig is volgens de AVG.

2.4 Rollen en verantwoordelijkheden

Het CMT/de directie is ambtelijk gezien eindverantwoordelijk voor het naleven van de privacywetgeving en het zorgvuldig omgaan met persoonsgegevens. Zij moeten kunnen aantonen dat de uitgangspunten en kaders in de praktijk worden toegepast. Privacy is echter niet alleen een taak van de directie: ook het management en iedere medewerker van provincie Gelderland draagt hier verantwoordelijkheid voor.

Het CMT/directie:

- Is eindverantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens binnen de provincie;
- Moet kunnen aantonen dat de verwerking voldoet aan de privacywetgeving;
- Laat kaders en beleid opstellen voor de bescherming van persoonsgegevens;
- Stuurt op de uitvoering van dit beleid en beoordeelt de risico's;
- Ziet erop toe dat de genomen maatregelen voldoende bescherming bieden;
- Betrekt de Functionaris Gegevensbescherming (FG) tijdig bij alle privacygerelateerde onderwerpen;
- Evalueert het privacybeleid minimaal één keer per jaar en stelt dit waar nodig bij.

Het management :

- Stelt, indien nodig, voor het eigen organisatieonderdeel specifieke privacykaders op en legt deze ter vaststelling voor aan de directie;
- Ziet toe op naleving van wetgeving, beleid en werkinstructies;
- Betrekt de centrale privacy ambassadeur van de afdeling, centrale privacy officers of de FG tijdig bij privacyvraagstukken;
- Maakt afspraken met andere organisatieonderdelen over het veilig delen van informatie;
- Kan onderdelen van de uitvoering mandateren aan programmamanagers, projectleiders of andere medewerkers.

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 functionaris gegevensbescherming (FG):

- Is een onafhankelijke toezichthouder binnen de provincie;
- Controleert of de provincie zich houdt aan de privacywetgeving en adviseert over verbeteringen;
- Rapporteert rechtstreeks aan de directie en, indien nodig, aan de Gedeputeerde Staten. Zie paragraaf ook paragraaf 2.3.5 voor de taken en verantwoordelijkheden van de FG.

De Privacy Officers:

- Vormen samen (met privacy ambassadeurs en Chief privacy officer) het privacyteam van provincie Gelderland.
- Adviseren afdelingen over de toepassing van de AVG en andere privacywetgeving.
- Helpen bij het uitvoeren van (pre-)DPIA's, verwerkersovereenkomsten, privacytoetsen en gegevensleveringen.

- Stellen centrale beleidsstukken, richtlijnen, procedures en formats op.
- Houden toezicht op de naleving van het privacybeleid en bewaken de voortgang van verbeteracties.
- Beoordelen meldingen van mogelijke datalekken, adviseren over vervolgstappen en coördineren de afhandeling en registratie in Trustbound.
- Analyseren datalekken en signaleren structurele risico's of verbeterpunten.
- Geven cursussen, presentaties en trainingen om het privacybewustzijn te vergroten.
- Zorgen dat nieuwe ontwikkelingen op het gebied van privacy en gegevensbescherming binnen de organisatie worden gedeeld.
- Onderhouden contact met de FG, de CISO en andere beleidsteams om beleid, informatiebeveiliging en uitvoering goed op elkaar af te stemmen.
- Ondersteunen en coachen de privacy-ambassadeurs bij vragen, signalen en complexe casussen.
- Adviseren de directie en het management over privacyrisico's, naleving en verbeterpunten.

Chief Privacy Officer (CPrO)

- Bewaakt de samenhang en koers van het privacybeleid op strategisch niveau.
- Stimuleert en coördineert samenwerking tussen de privacyrollen en andere beleidsterreinen.
- Adviseert de directie over de strategische ontwikkeling van privacy binnen de organisatie.

De Privacy Ambassadeurs:

- Zijn het eerste aanspreekpunt binnen hun afdeling voor vragen over privacy.
- Bevorderen een zorgvuldige omgang met persoonsgegevens.
- Signaleren risico's en bespreken deze met de centrale privacy officers.
- Betrekken de FG wanneer dat nodig is.
- Helpen bij DPIA's, verwerkersovereenkomsten, datalekken en het bijhouden van het verwerkingsregister.
- Bevorderen bewustwording over privacy binnen hun afdeling.

Chief Information Security Officer (CISO)

- Is verantwoordelijk voor het opstellen en uitvoeren van het informatiebeveiligingsbeleid.
- Houdt toezicht op de naleving van dit beleid.
- Werkt samen met het privacyteam, omdat informatiebeveiliging en privacy sterk met elkaar samenhangen.

De concretisering van de privacy rollen in de organisatie binnen provincie Gelderland is gevisualiseerd in de **RACI-matrix**, zoals opgenomen in de processen in de bijlagen.

2.5 Uitwerking en evaluatie

Dit privacybeleid werkt volgens de Plan-Do-Check-Act-cyclus: plannen, uitvoeren, controleren en verbeteren. Op deze manier blijft privacy en gegevensbescherming actueel en goed geborgd binnen de organisatie. De Functionaris Gegevensbescherming (FG) houdt toezicht op de uitvoering en rapporteert hierover aan de algemeen directeur.

2.6 Bewustwording

Provincie Gelderland 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. De FG wordt om inbreng gevraagd bij privacy bewustwordingsprogramma's.

2.7 Privacybeleid per afdeling

De uitgangspunten en verplichtingen uit dit privacybeleid gelden voor alle afdelingen van provincie Gelderland. Afdelingen kunnen, waar nodig, aanvullende werkafspraken of procedures maken die aansluiten op hun eigen taken.

2.8 Inwerkingtreding

Dit privacybeleid treedt in werking nadat het formeel is vastgesteld door de directie (onderdeel van het CMT) en met instemming van de ondernemingsraad (OR).