

Privacybeleid Provincie Limburg 2025

Gedeputeerde Staten van Limburg maken ter voldoening aan het bepaalde in artikel 24, tweede lid, van de Algemene verordening gegevensbescherming en artikel 4a van de Wet politiegegevens bekend dat zij in hun vergadering van 17 december 2024 hebben vastgesteld:

Privacybeleid Provincie Limburg 2025

1. Inleiding

Binnen de Provincie Limburg worden verschillende persoonsgegevens verwerkt (bijvoorbeeld van burgers en medewerkers). Persoonsgegevens worden voornamelijk verzameld van burgers voor het goed kunnen uitvoeren van wettelijke en/of autonome taken of vanwege een andere legitieme noodzaak die verband houdt met de kwaliteit en continuïteit van de provinciale bedrijfsvoering. Tegelijkertijd gaat ook de Provincie Limburg mee met nieuwe ontwikkelingen zoals nieuwe en innovatieve technologieën, globalisering. Tevens stelt een steeds verdere digitalisering van de overheid andere eisen aan de bescherming van gegevens en privacy. De Provincie Limburg is zich hier bewust van en streeft ernaar dat de privacy gewaarborgd blijft, onder andere door het treffen van maatregelen op het gebied van informatiebeveiliging, dataminimalisatie en transparantie. Een burger moet erop kunnen vertrouwen dat de Provincie Limburg zorgvuldig en veilig met persoonsgegevens omgaat.

Tevens worden er binnen de Provincie Limburg politiegegevens verwerkt door de buitengewoon opsporingsambtenaren (boa's) in het kader van de strafrechtelijke handhaving. Op de verwerking van politiegegevens is de Wet politiegegevens (hierna: Wpg) van toepassing en niet de Algemene verordening gegevensbescherming (hierna: AVG). Daarnaast zijn er ook een aantal andere regelingen van toepassing op de verwerking van politiegegevens, zoals het Besluit politiegegevens (hierna: Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren (hierna: Bpg boa) en de Regeling periodieke audit politiegegevens. Het college van Gedeputeerde Staten van Limburg is als werkgever verwerkingsverantwoordelijke in het kader van de Wpg.

Dit privacybeleid is een uitwerking van artikel 24, tweede lid van de AVG en heeft tot doel te laten zien welke maatregelen de Provincie Limburg heeft genomen om aan te tonen dat de persoonsgegevens in overeenstemming met de toepasselijke wet- en regelgeving worden verwerkt. Dit beleid is van toepassing op de hele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de Provincie Limburg. Daarnaast beschrijft dit beleid hoe de Provincie Limburg binnen de wettelijke kaders van de Wpg en onderliggende regelgeving met politiegegevens omgaat. De boa's van de Provincie Limburg zijn zich ervan bewust dat zij zorgvuldig moeten omgaan met politiegegevens. Zij worden daarin getraind en volgen interne werkinstructies. Het geautomatiseerde systeem waarmee zij politiegegevens verwerken, zorgt ervoor dat de verwerking op rechtmatige wijze plaatsvindt.

2. Wetgeving en definities

Iedereen heeft recht op bescherming van zijn persoonlijke levenssfeer. Dit recht is geborgd in de Grondwet en is een groot goed. Het juridische kader voor de omgang met persoonsgegevens in Nederland staat in de AVG, de Uitvoeringswet AVG, de Wpg en diverse andere wetten (bijvoorbeeld de Kieswet en de Archiefwet). Bij de omgang met persoonsgegevens hanteert en toetst de Provincie Limburg met name de regels uit de AVG en Wpg. Sectorspecifieke privacywetgeving die van toepassing is op de verwerking van persoonsgegevens door de Provincie Limburg wordt in een separaat register opgenomen.

De volgende begrippen worden in de AVG (artikel 4, van de AVG) en Wpg (artikel 1, van de Wpg) gebruikt en zijn van belang voor een goed begrip van deze Europese verordening, Nederlandse wetgeving en onderhavig beleid:

- **Autoriteit Persoonsgegevens:** de onafhankelijke toezichthouder die toeziet op de naleving van de privacy wet- en regelgeving;
- **Betrokkene:** de persoon op wie de persoonsgegevens/politiegegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt;
- **Gegevensbeschermingseffectbeoordeling/data protection impact assessment (DPIA):** een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen om 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

- of politiegegevens en is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen. De beoordeling bevat ten minste een inschatting van de risico's van de verwerking en de vereiste beheersmaatregelen om tekortkomingen op te lossen;
- **Persoonsgegevens:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Het gaat hierbij om ieder gegeven dat direct 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;
 - **Politiegegevens:** elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaken, bedoeld in de artikelen 3 en 4 van de Politiewet 2022, met uitzondering van (1) de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften of (2) de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1° en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012;
 - **Verwerker:** de persoon of organisatie die de persoonsgegevens of politiegegevens verwerkt in opdracht van een andere persoon of organisatie;
 - **Verwerking:** een verwerking is elke handeling of geheel van handelingen met betrekking tot persoonsgegevens of politiegegevens oftewel alles wat je met persoonsgegevens doet, zoals: lezen, vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander en vernietigen;
 - **Verwerkingsverantwoordelijke:** een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens of politiegegevens vaststelt.

3. Organisatie: taken en verantwoordelijkheden

3.1. Centrale verantwoordelijkheid

Het college van Gedeputeerde Staten van de Provincie Limburg (hierna: 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 of politiegegevens.

Het college van Gedeputeerde Staten legt over de uitvoering van het privacybeleid verantwoording af aan Provinciale Staten van de Provincie Limburg (hierna: Provinciale Staten) en betracht beleidstransparantie met behulp van publieksvoorlichting. Als verantwoordelijk gezag stelt het college van Gedeputeerde Staten privacybeleid op, draagt het dit uit en wijst het taken, verantwoordelijkheden en bevoegdheden toe.

3.2. Rollen (functies) rondom privacy en informatiebeveiliging

3.2.1. De secretaris/algemeen directeur

De secretaris/algemeen directeur is verantwoordelijk voor de kaderstelling en sturing op de uitvoering van het privacybeleid. Minimaal één keer per jaar evalueert hij/zij, samen met de functionaris voor gegevensbescherming (hierna: FG) de naleving van privacyregelgeving en onderhavig beleid. Daarnaast zorgt hij/zij ervoor dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens of politiegegevens.

3.2.2. Het management

De clustermanagers zijn op uitvoeringsniveau verantwoordelijk voor een privacybestendige bedrijfsvoering en gegevensuitwisseling met derden. Uiteraard voor zover passend binnen hun mandaat en de door het college van Gedeputeerde Staten vastgestelde beleidskaders. De clustermanagers leggen hierover via de directie verantwoording af aan het college van Gedeputeerde Staten. Daarnaast kan het voorkomen dat ook een directeur of programma-/projectmanager op uitvoeringsniveau verantwoordelijk is voor een proces waarin persoonsgegevens worden verwerkt. De clustermanagers winnen advies in bij de Privacy-officer of privacyrechtjurist(en) voordat wordt aangevallen met een nieuwe of verdere verwerking van persoonsgegevens.

3.2.3. Het privacy- en informatiebeveiligingsteam (PIT)

Privacybescherming vergt kennis op het gebied van gegevensmanagement en IT, juridische kennis van wet- en regelgeving, auditexpertise voor de DPIA's, kennis van informatiebeveiliging en van werkprocessen en systemen. Binnen de Provincie Limburg is een team actief waarin deze expertise voorhanden is. Dit team heet 'privacy- en informatiebeveiligingsteam', kortweg: PIT. Het PIT ondersteunt de clustercoördinatoren privacy, de clustermanagers, de directie en het college van Gedeputeerde Staten bij de uitvoering van het privacybeleid. Dit team bestaat ten minste uit de Privacy-officer (jurist van het cluster Algehele Juridische Zaken (AJZ)), privacyrechtjurist(en), de Information Security Officer (senior Adviseur Organisatie en Informatie van het cluster Organisatie en Informatie) en de FG (als adviseur). Dit team adviseert de directie eveneens bij datalekken.

Concreet heeft het PIT de volgende taken:

- advisering over uitvoering en actualisatie provinciaal privacybeleid;
- signaleren van privacyrisico's;
- ondersteuning management en bestuur bij privacyvraagstukken;
- implementeren (nieuwe) privacywetgeving;
- doen van aanbevelingen op het gebied van privacy en informatiebeveiliging;
- vertaling adviezen en bevindingen van de FG in concrete actiepunten en uitvoering hiervan binnen de (met de directie) afgesproken termijnen.

3.2.4. De clustercoördinatoren privacy

Elke clustermanager wijst een medewerker aan die binnen zijn cluster fungeert als privacy-coördinator. Deze coördinator is het eerste aanspreekpunt voor het PIT bij de implementatie van (nieuwe) maatregelen op het terrein van privacy en heeft verder de volgende taken en verantwoordelijkheden:

- draagt mede zorg voor het bewustwordingsproces rondom privacy en informatiebeveiliging binnen zijn/haar cluster;
- heeft een proactieve rol in het signaleren of er sprake is van een nieuwe verwerking en of het noodzakelijk is dat daarvoor een verwerkersovereenkomst moet worden afgesloten;
- het actueel houden van verwerkingen binnen het cluster;
- het doorgeven van nieuwe verwerkingen en wijzigingen in verwerkingen van persoonsgegevens aan de Privacy-officer en of privacyrechtjurist(en) voor opname in respectievelijk wijziging van het register van verwerkingen;
- het deelnemen aan activiteiten die door het PIT worden georganiseerd over actualiteiten op het gebied van privacy.

3.2.5. De FG

De Provincie Limburg heeft een FG aangesteld. De FG is 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 AVG en Wpg. Deze functionaris is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens en politiegegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en het provinciale beleid op het gebied van privacy. Concreet heeft de FG de volgende taken:

- informeren en adviseren van de verwerkingsverantwoordelijke en hun medewerkers over hun verplichtingen uit de AVG, Wpg en andere relevante privacywetgeving;
- toezien op de naleving van de AVG, Wpg, andere relevante privacywetgeving en het provinciale privacybeleid, waaronder bewustmaking en voorlichting van betrokken medewerkers;
- adviseren over DPIA's en toezien op de uitvoering daarvan;
- samenwerken met toezichthoudende autoriteiten (zoals de Autoriteit Persoonsgegevens) en optreden als provinciaal contactpunt voor toezichthoudende autoriteiten;
- helpen privacyklachten tot een goed einde te brengen (ombudsfunctie);
- bij privacy-incidenten adviseren over ernst en omvang;
- toezien op het register van verwerkingsactiviteiten;
- advieslid van het PIT.

De FG krijgt de nodige ruimte voor professionele uitvoering van zijn taken. Conform artikel 38, van de AVG en artikel 36, van de Wpg:

- zorgen het college van Gedeputeerde Staten en de clustermanagers en project-/programmamanagers ervoor dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens of politiegegevens;
- wordt de FG bij de vervulling van zijn taken ondersteund door hem toegang te verschaffen tot persoonsgegevens of politiegegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken;
- wordt de FG niet geïnstrueerd over de invulling van taken of gestraft of ontslagen voor de uitvoering van zijn taken;
- is de zienswijze van de FG zwaarwegend bij de naleving van privacywetgeving door de Provincie Limburg.

Elk kwartaal brengt de FG verslag uit van zijn/haar werkzaamheden aan de secretaris/algemeen directeur en de CIO.

3.2.6. De bevoegd functionaris

Voor verwerkingen conform artikel 9 van de Wpg is het noodzakelijk om een bevoegd functionaris aan te wijzen. De bevoegd functionaris is de 'hoeder' van de gegevens die onder artikel 9 van de Wpg

worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Bpg. De bevoegd functionaris wordt door de werkgever aangewezen via een separaat aanwijzingsbesluit. De Provincie Limburg heeft twee bevoegd functionarissen aangewezen.

De bevoegd functionaris heeft onder andere de volgende taken:

- het doel van de artikel 9 Wpg-verwerking omschrijven en vastleggen;
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd;
- bewaken dat gegevens rechtmatig worden verkregen en verwerkt. Hierbij moet vooral worden gelet op de termijnen.

Functie/rol	Taken/verantwoordelijkheid
Het college van Gedeputeerde Staten	Eindverantwoordelijk voor het privacybeleid en het waarborgen van de privacy van betrokkenen.
Secretaris/algemeen directeur	Verantwoordelijk voor kaderstelling en sturing met betrekking tot het privacybeleid.
Cluster-/project/-programmamanagers	Uitvoering en controle op naleving privacybeleid.
Functionaris Gegevensbescherming	Controle op naleving en advisering op het gebied van privacy.
PIT	Ondersteuning en advisering bestuur, de clustercoördinatoren privacy en het management op het terrein van bescherming van persoonsgegevens en uitvoering van het Provinciale privacybeleid.
Privacy-officer	Advisering over en implementatie privacybeleid en –wetgeving. Actueel houden register van verwerkingsactiviteiten.
Clustercoördinatoren privacy	Informatieverstrekking, bewustwording en cluster specifieke taken op het gebied van privacy.
Bevoegd functionaris	Hoeder van de gegevens die op grond van artikel 9, van de Wpg worden verwerkt

Schematische weergave taken en verantwoordelijkheden op terrein van privacy

4. Uitgangspunten en maatregelen

4.1. Algemeen

In dit hoofdstuk staan de uitgangspunten en maatregelen centraal die de Provincie Limburg hanteert bij de verwerking van persoonsgegevens en politiegegevens. Zoals eerder aangegeven, wordt bij het bepalen van een passende maatregel o.a. rekening gehouden met de soort verwerking (de aard, omvang, context, het doel) en de risico's voor betrokkenen (hoe groot is de kans dat zich ook daadwerkelijk een schending van de privacy van betrokkene(n) voordoet en als dat onverhoopt mocht gebeuren, hoeveel hinder en schade heeft dit dan voor hem/haar).

4.1.1. AVG

De Provincie Limburg hanteert voor het op de juiste manier waarborgen van privacy het 'Borgingsproduct Gegevensbescherming' van de VNG/ Informatiebeveiligingsdienst (IBD). Het borgingsproduct is een hulpmiddel om de AVG te vertalen naar een kwaliteitscyclus voor gegevensbescherming voor gemeentelijke processen. Gezien de opzet van dit borgingsproduct is het ook geschikt voor de provinciale processen.

4.1.2. Wpg

Aanvullend op de normen uit de AVG gelden op grond van de Wpg de volgende eisen:

- gegevens die op feiten zijn gebaseerd zijn gescheiden van gegevens die op een persoonlijk oordeel zijn gebaseerd;
- er wordt onderscheid gemaakt tussen verschillende categorieën betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- via geautomatiseerde systemen wordt de invoer van gegevens gelogd;
- er gelden specifieke termijnen voor het bewaren, verwijderen en vernietigen van politiegegevens.

Deze eisen zijn geborgd binnen het Boa Registratie Systeem (hierna: BRS) waarin boa's de politiegegevens verwerken.

4.2. Doeleinden

Volgens de AVG en Wpg mogen persoonsgegevens of politiegegevens alleen verwerkt worden als daarvoor een doel is vastgesteld. Het doel moet per individuele verwerking uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doeleinden verwerkt worden, tenzij er sprake is van een verenigbaar doel. Voor de uitvoering van diverse provinciale taken zijn de doeleinden voor het verwerken in een wet vastgelegd, net als de persoonsgegevens of politiegegevens die gevraagd en verwerkt mogen worden. Op het moment dat een verwerking wordt opgenomen in het register zoals genoemd onder punt 4.14, wordt het doel van de verwerking hierin vermeld.

Binnen de Provincie Limburg worden persoonsgegevens of politiegegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen verzameld en verwerkt. Bij opname van de verwerking in het register ex artikel 30, van de AVG of artikel 31, van de Wpg (verwerkingenregister) wordt dit doel vermeld.

4.3. Grondslag

Persoonsgegevens en politiegegevens mogen niet alleen worden verwerkt als daarvoor een doel is vastgesteld, er moet daarnaast ook een beroep kunnen worden gedaan op een grondslag voor de verwerking.

4.3.1. AVG

In artikel 6 van de AVG zijn zes grondslagen vastgelegd voor de verwerking van persoonsgegevens. Voor de verwerking van persoonsgegevens moet op ten minste één van de zes grondslagen een beroep worden gedaan. Het betreft de volgende grondslagen:

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- de verwerking is noodzakelijk ter bescherming van de vitale belangen (de verwerking is noodzakelijk voor de betrokkene zijn leven of gezondheid);
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waar de betrokkene onderdeel van is;
- de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- de gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen (geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun publieke taken).

4.3.2. Wpg

De Wpg onderscheidt verschillende grondslagen waarvoor politiegegevens mogen worden verwerkt. Deze staan in de artikelen 8, 9, 10, 12 en 13, van de Wpg beschreven. Het Bpg boa beschrijft in artikel 2 dat voor de boa alleen artikel 8, 9 en 13 Wpg-verwerkingen van toepassing zijn. Afhankelijk van de grondslag gelden er andere voorwaarden, bijvoorbeeld voor de verwerkingstermijn en toegankelijkheid voor andere opsporingsambtenaren. Het betreft de volgende grondslagen:

- Artikel 8 van de Wpg: politiegegevens kunnen worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak.
- Artikel 9 van de Wpg: politiegegevens kunnen worden verwerkt die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen.
- Artikel 13 van de Wpg: ten behoeve van ondersteuning van de taak mogen politiegegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9 Wpg verder worden verwerkt voor zover zij relevant zijn.

De grondslag dient te worden vastgelegd in het register van verwerkingsactiviteiten.

De Provincie Limburg verwerkt alleen persoonsgegevens en politiegegevens indien een rechtmatige grondslag van toepassing is. De grondslag wordt vastgelegd in het verwerkingenregister.

4.4. Dataminimalisatie

Bij de verwerking van persoonsgegevens of politiegegevens blijft de hoeveelheid en het soort gegevens beperkt (artikel 5 onder c van de AVG of artikel 4, van de Wpg): er worden zo min mogelijk persoonsgegevens verwerkt, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt.

De Provincie Limburg controleert bij aanvang en gedurende de verwerking van persoonsgegevens of politiegegevens of het doel niet met minder, alternatieve of andere gegevens kan worden bereikt.

4.5. Bewaartermijnen

4.5.1. AVG

Persoonsgegevens mogen niet langer bewaard worden dan strikt noodzakelijk voor het doel waarvoor ze zijn verzameld, de dienstverlening of wettelijke verplichting.

Er is op grond van de AVG geen concrete bewaartermijn voor persoonsgegevens. Persoonsgegevens mogen echter alleen bewaard worden als identificeerbare gegevens, voor zolang het nodig is voor de doeleinden waarvoor ze verzameld zijn. Bij de bepaling van de bewaartermijn is het dus zaak om na te gaan hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld of worden gebruikt. Wel zijn er concrete bewaartermijnen in andere wetten waar organisaties zich aan moeten houden, bijvoorbeeld in de Archiefwet en de belastingwetgeving.

4.5.2. Wpg

In de Wpg staan termijnen voor het bewaren van politiegegevens. Politiegegevens die op grond van artikel 8 en 9, van de Wpg zijn verwijderd, worden gedurende vijf jaar bewaard voor het afhandelen van klachten en het verantwoorden van verrichtingen (audits). Verder kunnen deze gegevens in bijzondere gevallen en voor zover dat noodzakelijk is voor een artikel 9-verwerking ter beschikking worden gesteld voor hernieuwde verwerking. Dit kan alleen in opdracht van de Officier van Justitie. Deze gegevens mogen ook worden verwerkt ten behoeve van wetenschappelijk onderzoek en statistiek.

De Provincie Limburg stelt voor iedere verwerking de (wettelijke) bewaartermijnen van persoonsgegevens of politiegegevens vast en neemt maatregelen om persoonsgegevens tijdig te verwijderen, vernietigen of te anonimiseren. Bewaartermijnen worden vastgelegd in het verwerkingenregister.

4.6. Data-integriteit

De AVG en Wpg eisen dat maatregelen worden getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn. Indien nodig worden persoonsgegevens geactualiseerd. De AVG en Wpg geven in dit kader aan dat alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

De Provincie Limburg neemt alle redelijke maatregelen om te borgen dat persoonsgegevens en politiegegevens juist en actueel zijn.

4.7. Beveiliging

Verantwoord omgaan met persoonsgegevens of politiegegevens valt of staat met een adequate beveiliging van de gegevens. Slechte beveiliging kan bijvoorbeeld leiden tot een datalek, verandering van, en ontoegankelijkheid van persoonsgegevens. Op grond van de AVG en Wpg moeten bedrijven en overheden dan ook passende technische en organisatorische maatregelen nemen. Er moet dus niet alleen naar de techniek worden gekeken, maar ook naar hoe de Provincie Limburg als organisatie met persoonsgegevens of politiegegevens omgaat. Zo moet bijvoorbeeld worden bekeken wie er toegang heeft tot welke gegevens.

De Provincie Limburg zorgt voor een passende beveiliging van persoonsgegevens en politiegegevens conform het vigerende informatiebeveiligingsbeleid.

4.8. Transparantie

4.8.1. Informatieplicht

4.8.1.1 AVG

In de AVG is expliciet opgenomen dat persoonsgegevens verwerkt moeten worden op een manier die transparant is voor de betrokkene. Voor een natuurlijke persoon moet transparant zijn of en in hoeverre zijn persoonsgegevens (zullen) worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt: het transparantiebeginsel (artikel 5, eerste lid onder a van de AVG). Dit betekent dat een betrokkene onder

andere op de hoogte moet worden gesteld van de verwerking van zijn/haar persoonsgegevens en de doeleinden hiervan. Deze actieve informatieplicht is vastgelegd in artikel 13, eerste lid en artikel 14, eerste lid van de AVG. Communicatie met betrokkene dient bovendien plaats te vinden in begrijpelijke, beknopte en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal (artikel 12, eerste lid van de AVG).

De Provincie Limburg informeert betrokkene actief over het verwerken van zijn/haar persoonsgegevens. Wanneer betrokkenen gegevens aan de Provincie Limburg verstrekken, worden zij op dat moment (bijvoorbeeld via het aanvraagformulier) op de hoogte gesteld van de manier waarop de Provincie Limburg met hun persoonsgegevens om zal gaan. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de Provincie Limburg persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene binnen een redelijke termijn geïnformeerd: altijd direct de eerste keer dat met hem/haar wordt gecommuniceerd en uiterlijk binnen een maand. Deze plicht is niet van toepassing als betrokkene die informatie al heeft, het onmogelijk of ondoenlijk is om de informatie te verstrekken, de verwerking wettelijk verplicht is of daarmee de doeleinden van de verwerking ernstig in het gedrang komen.

4.8.1.2 Wpg

De verwerkingsverantwoordelijke heeft op grond van de Wpg ook een informatieplicht. De verwerkingsverantwoordelijke verstrekt aan de betrokkene informatie over de verwerking van politiegegevens in een beknopte en toegankelijke vorm en in duidelijke en eenvoudige taal. De informatie wordt met passende middelen, waaronder elektronische middelen, verstrekt en in beginsel in dezelfde vorm als de vorm van het verzoek. De volgende informatie dient aan de betrokkene te worden verstrekt:

- de identiteit en contactgegevens van de verwerkingsverantwoordelijke en de FG;
- de verwerkingsdoelen van de politiegegevens;
- de rechten van betrokkene;
- het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

In specifieke gevallen verstrekt de verwerkingsverantwoordelijke de volgende informatie aan de betrokkene:

- de rechtsgrondslag van de verwerking;
- de bewaartermijn van de politiegegevens;
- indien noodzakelijk, extra informatie, in het bijzonder wanneer de politiegegevens zonder medeweten van de betrokkene worden verzameld;
- het bestaan van geautomatiseerde besluitvorming en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

In het geval er sprake is van een kennelijk ongegrond of buitensporig verzoek, kan de verwerkingsverantwoordelijke weigeren gevolg te geven aan het verzoek

De Provincie Limburg maakt niet alleen op een transparante manier duidelijk of zij persoonsgegevens en politiegegevens verwerkt en hoe zij de privacy te allen tijde probeert te waarborgen, zij informeert betrokkene – behoudens een aantal wettelijke uitzonderingen – ook actief over de verwerking van zijn/haar gegevens.

4.8.2. Rechten van betrokkenen

4.8.2.1 AVG

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 informatie:* betrokkenen hebben het recht om aan de Provincie Limburg te vragen of zijn/haar persoonsgegevens worden verwerkt.
- *Inzagerecht:* betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar persoonsgegevens worden verwerkt.
- *Recht op rectificatie:* als blijkt dat de persoonsgegevens die worden verwerkt niet correct of incompleet zijn, kan de betrokkene een verzoek bij de Provincie Limburg indienen om deze gegevens te corrigeren of aan te vullen.

- *Recht op beperking*: betrokkenen kunnen aan de Provincie Limburg verzoeken om de verwerking van hun persoonsgegevens tijdelijk stop te laten zetten.
- *Recht op gegevenswissing*: in een aantal gevallen kan de betrokkene aan de Provincie verzoeken dat zijn/haar persoonsgegevens worden verwijderd.
- *Recht op bezwaar*: betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens.

4.8.2.2 Wpg

De rechten op grond van de Wpg zijn grotendeels hetzelfde als de rechten op grond van de AVG. Toch wijken zij op een aantal punten ook af van de AVG. Betrokkenen hebben het recht om de politiegegevens die de Provincie Limburg onder de Wpg verwerkt, in te zien.

Als politiegegevens onder de Wpg onjuist of onvolledig zijn, dan kunnen betrokkenen de Provincie Limburg verzoeken de politiegegevens aan te passen. Daarnaast kunnen betrokkenen verzoeken de politiegegevens te laten verwijderen of vragen om een beperking van de verwerking van de politiegegevens.

De Provincie heeft het recht om een verzoek af te wijzen als:

- het verzoek gerechtelijke onderzoeken of procedures zou belemmeren;
- dit nadelige gevolgen heeft voor het voorkomen van het begaan van strafbare feiten, voor opsporing, onderzoek, vervolging of het opleggen van straffen;
- de openbare veiligheid in het geding is;
- de rechten en vrijheden van derden worden geschonden;
- de nationale veiligheid in het geding is;
- de Provincie de wettelijke plicht heeft deze politiegegevens gegevens te bewaren;
- het kennelijk een ongegrond of buitensporig verzoek is.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen bij de Provincie Limburg. Dit verzoek kan zowel schriftelijk als digitaal ingediend worden. De Provincie Limburg moet binnen één maand na ontvangst van het verzoek, de betrokkene informeren over de uitvoering van het verzoek. Binnen één maand dient de Provincie Limburg aan te geven of zij wel of geen gehoor geeft aan het verzoek. Als er geen gehoor wordt gegeven aan het verzoek, kan betrokkene bezwaar (ex artikel 7:1 Algemene wet bestuursrecht) maken bij de Provincie Limburg, of een klacht in te dienen bij de Autoriteit Persoonsgegevens.

De Provincie Limburg informeert betrokkenen over hun rechten en draagt er zorg voor dat betrokkenen op een laagdrempelige wijze hiervan gebruik kunnen maken.

4.9. Geautomatiseerde verwerkingen

4.9.1. Profilerings

Wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen, spreken we van profilering. Voorbeelden van persoonlijke aspecten kunnen zijn: financiële situatie, interesses, gedrag of locatie.

De Provincie Limburg doet niet aan louter geautomatiseerde besluitvorming of profilering welke herleidbaar is tot het individu.

4.9.2. Inzet van camera's

Ter vergroting van de veiligheid (bescherming medewerkers en bezoekers, tegengaan van diefstal en beschadiging van provinciale eigendommen) wordt in en rondom het Provinciehuis gebruik gemaakt van cameratoezicht. De camerabeelden worden alleen voor dat doeleinde gebruikt. Camera's kunnen een grote inbreuk maken op de privacy van diegene die wordt gefilmd. Om de privacy zo goed mogelijk te waarborgen zal de Provincie Limburg op duidelijke wijze (o.a. in een protocol cameratoezicht en via bebording) kenbaar maken dat er sprake is van cameratoezicht.

De Provincie Limburg maakt ter vergroting van de veiligheid in en rondom het Provinciehuis gebruik van cameratoezicht. Bezoekers van het Provinciehuis worden hier o.a. met behulp van borden op gewezen.

4.10. Verwerkingenregister

De Provincie Limburg is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de Provincie Limburg de verwerkingsverantwoordelijke of verwerker is, het zogenaamde verwerkingenregister. Dit register bevat:

- de naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- de doelen van de verwerking;
- de grondslag van de verwerking
- een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- een beschrijving van de ontvangers van de persoonsgegevens;
- een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- de bewaartermijnen;
- een algemene beschrijving van de beveiligingsmaatregelen.

De Wpg verplicht ook tot het bijhouden van een verwerkingenregister. Aanvullend op het verwerkingenregister op grond van de AVG moet in het verwerkingenregister op grond van de Wpg nog de volgende informatie worden opgenomen:

- in voorkomend geval: het gebruik van profilering;
- de toekenning van autorisaties.

De Privacy-officer binnen het cluster AJZ en de privacyrechtjuristen beheren het register. De clusters, programma's en projecten dienen nieuwe verwerkingen - voor opname in het register - en wijzigingen in bestaande verwerkingen tijdig aan te leveren bij voornoemde medewerkers van AJZ. Hierbij kunnen ze gebruik maken van het inventarisatieformulier 'nieuwe verwerking persoonsgegevens'. Eén keer per jaar richt het cluster AJZ zich actief tot de clustercoördinatoren van alle clusters met het verzoek om de verwerkingen binnen hun cluster te (laten) controleren op actualiteit en indien nodig aan te passen en/of aan te vullen met eventuele nieuwe verwerkingen.

De Provincie Limburg houdt een register bij waarin de verwerkingsactiviteiten worden vastgelegd. Dit verwerkingenregister wordt periodiek geactualiseerd.

4.11. De verwerkersovereenkomst

De Provincie Limburg besteedt de verwerking van persoonsgegevens of politiegegevens ook uit aan derden. Als verwerkingsverantwoordelijke mag de Provincie Limburg niet zomaar met een verwerker in zee gaan. Zij moet vaststellen of de verwerker voldoet aan de AVG of Wpg. Meer concreet: de verwerker moet passende technische en organisatorische maatregelen treffen zodat deze voldoet aan de AVG of Wpg en de rechten van betrokkenen voldoende gewaarborgd zijn.

Alle maatregelen die de verwerker hiervoor dient te nemen, komen vast te liggen in een zogenaamde verwerkersovereenkomst tussen de Provincie Limburg en de verwerker. Binnen de Provincie Limburg wordt gewerkt met een standaard verwerkersovereenkomst. De vraag of een verwerkersovereenkomst noodzakelijk is, maakt bovendien onderdeel uit van de interne inkoop-/aanbestedingsprocedure. De manager van het cluster die de opdracht aan een derde verstrekt voor de verwerking van persoonsgegevens of politiegegevens is tevens verantwoordelijk voor het afsluiten van de verwerkersovereenkomst.

De Provincie Limburg houdt een register bij van verwerkersovereenkomsten.

De Provincie Limburg zal bij iedere nieuwe en of bestaande dienst waarbij opdracht is of wordt verstrekt voor verwerking van persoonsgegevens of politiegegevens zeker stellen dat de verwerker en/of medeverantwoordelijke voldoende maatregelen heeft getroffen, waardoor de Provincie Limburg haar verantwoordelijkheid kan nemen. De details en eisen die gesteld worden aan de verwerking door verwerkers en medeverantwoordelijke zullen eenduidig worden vastgelegd in een verwerkersovereenkomst.

4.12. Het ter beschikking stellen en verstrekken van politiegegevens

De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en heverstrekken ervan. Het ter beschikking stellen van politiegegevens vindt plaats binnen het Wpg-domein. Dit houdt in dat politiegegevens kunnen worden gedeeld met andere opsporingsambtenaren (boa's, medewerkers van de politie of de Koninklijke Marechaussee) die deze gegevens nodig hebben voor hun taken. Hierbij vindt een afweging plaats op basis van noodzakelijkheid, proportionaliteit (het middel moet in verhouding staan tot het doel) en subsidiariteit (het minst ingrijpende middel moet worden gehanteerd om het doel te bereiken).

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval mogen politiegegevens alleen worden verstrekt aan personen of instanties buiten het Wpg-domein, voor zover dit noodzakelijk is voor de doeleinden zoals vermeld in de Wpg en het Bpg. Het gaat bijvoorbeeld om verstrekkingen aan een toezichthouder, een advocaat of de belastingdienst. Voor het verstrekken van gegevens geldt een documentatieplicht. Bij dergelijke verstrekkingen wordt altijd vooraf getoetst of de verstrekking voldoet aan de wetgeving. De Provincie Limburg verstrekt geen politiegegevens aan ontvangers in andere landen of internationale organisaties. De Provincie Limburg neemt ook niet deel aan samenwerkingsverbanden waarin politiegegevens worden gedeeld. Op het moment dat zij wel daartoe overgaat, handelt zij conform de geldende regels.

Verstrekkingen worden via het BRS geregistreerd en gedocumenteerd. Daarnaast maakt de Provincie Limburg gebruik van de landelijke verstrekkingenwijzer voor boa's. De verstrekkingenwijzer is specifiek opgesteld voor boa organisaties en geeft aan welke gegevens aan welke instanties mogen worden verstrekt en onder welke voorwaarden.

4.13. Gegevensbeschermingseffectbeoordeling/ data protection impact assessment (DPIA)

Een gegevensbeschermingseffectbeoordeling - ook wel data protection impact assessment (DPIA) genoemd - 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.

De Provincie Limburg moet dus zelf bepalen of er sprake is van een risicovolle verwerking. Bij de volgende categorieën verwerkingen moet de Provincie Limburg in ieder geval op grond van de AVG een DPIA uitvoeren:

- systematische, uitgebreide en geautomatiseerde beoordeling van persoonlijke aspecten van de betrokkenen (bijvoorbeeld: profilering);
- grootschalige verwerking van bijzondere gegevens;
- verwerking van strafrechtelijke gegevens;
- stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Verder zal de Provincie Limburg een DPIA uitvoeren indien er sprake is van hoge risico's voor de 'rechten en vrijheden' van betrokkenen.

Het besluit om een DPIA uit te voeren wordt genomen door de verantwoordelijke manager, na advies van de FG.

Bij risicovolle verwerkingen voert de Provincie Limburg een gegevensbeschermingseffect-beoordeling/DPIA uit. Dit geldt zowel op grond van de AVG als Wpg.

4.14. Datalekken

Er is sprake van een datalek als er een inbreuk plaatsvindt op de beveiliging van persoonsgegevens of politiegegevens, bijvoorbeeld als persoonsgegevens of politiegegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een ernstig datalek heeft plaatsgevonden meldt de Provincie Limburg dit zonder onredelijke vertraging, doch uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de AP. Als dit later dan 72 uur is, wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dat geval meldt de Provincie Limburg dit aan de betrokkenen in eenvoudige en duidelijke taal. Op deze mededelingsplicht zijn op grond van de Wpg enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd. Daarnaast wordt elk datalek geregistreerd in het datalekregister.

De Provincie Limburg heeft een Protocol melding datalekken. Bij de beslissing of een incident dat zich heeft voorgedaan moet worden gemeld bij de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene(n), moeten een aantal afwegingen worden gemaakt. In het protocol wordt toegelicht wat een datalek is, op welke wijze het datalek in de organisatie moet worden gemeld, hoe een datalek wordt afgehandeld en in welke gevallen en wanneer een datalek moet worden gemeld bij de Autoriteit persoonsgegevens en betrokkenen.

Zodra zich binnen de Provincie Limburg een ernstig datalek heeft voorgedaan, wordt dit direct gemeld bij de Autoriteit Persoonsgegevens.

4.15. Privacy by design en privacy by default

Privacybescherming bestaat niet alleen uit toetsing en controle achteraf. Ook aan de voorkant, bij het ontwerpen en inrichten van processen en systemen dient privacybescherming een belangrijk uitgangspunt te zijn. De adviseurs binnen het cluster Organisatie en Informatie hebben hierbij een ondersteunende en adviserende rol.

Voor de AVG en Wpg zijn privacy by design en privacy by default belangrijke onderdelen van de verantwoordingsplicht van de Provincie Limburg.

Privacy by design houdt in dat er al bij het ontwerpen van producten en diensten voor wordt gezorgd dat persoonsgegevens of politiegegevens 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 gegevens te beschermen. Dataminimalisatie is een ander voorbeeld van één van de uitgangspunten die gehanteerd worden: zo min mogelijk persoonsgegevens of politiegegevens verzamelen, alleen datgene wat strikt noodzakelijk is voor het bereiken van het doel.

Privacy by default betekent dat de standaardinstellingen van diensten of invulformulieren altijd zoveel mogelijk de privacy moeten garanderen. Bijvoorbeeld door een app die de Provincie Limburg aanbiedt niet de locatie van gebruikers te laten registreren als dat niet nodig is of door iemand die zich op een nieuwsbrief wil abonneren alleen te vragen naar zijn/haar emailadres.

Bij (verlening van opdrachten voor) de ontwikkeling van producten en diensten zal zoveel mogelijk rekening worden gehouden met privacy by design en privacy by default

5. Afsluiting

Het Privacybeleid Provincie Limburg 2025 kan worden aangehaald als Privacybeleid. Dit Privacybeleid wordt minimaal één keer per twee jaar geëvalueerd. Met het vaststellen van het Privacybeleid wordt het Privacybeleid Provincie Limburg 2018 ingetrokken.

Maastricht, d.d. 17 december 2024

Gedeputeerde Staten voornoemd

*de voorzitter,
E.G.M. Roemer*

*secretaris,
D.F. Timmer*