Privacyverklaring voor medewerkers

Interne verwerking van persoonsgegevens

versie 1, 2025 – tot heden

provincie Gelderland

Interne privacyverklaring voor medewerkers

Algemeen

Als werkgever vinden wij het belangrijk om zorgvuldig met jouw persoonsgegevens om te gaan en om jou daar helder over te informeren. In deze privacyverklaring leggen wij daarom uit welke gegevens wij gebruiken, waarom wij dat doen, hoe wij met jouw gegevens omgaan en welke rechten jij als medewerker hebt.

Wij werken voortdurend aan het verbeteren van onze informatiebeveiliging en privacybescherming. Dat betekent dat werkwijzen en systemen periodiek worden geëvalueerd en aangepast aan nieuwe wet- en regelgeving, technische ontwikkelingen en interne beleidskaders.

Welke persoonsgegevens verwerken we?

Wij verzamelen en verwerken (onder meer) de volgende persoonsgegevens:

Identificatie- en contactgegevens:
- NAW-gegevens;
- Leeftijdsgegevens;
- Contactgegevens;
- Nationaliteit, geslacht en burgerlijke staat;
- Identificatiegegevens;

Daarnaast worden van alle medewerkers die bij de provincie werkzaam zijn de basisgegevens, zoals naam, e-mailadres, afdeling/team, standplaats, functie en werkdagen, opgenomen in de Wie Is Wie. Dit systeem is bedoeld om collega's eenvoudig met elkaar in contact te brengen. Aanvullende gegevens, zoals een foto of telefoonnummer, kunnen op vrijwillige basis worden toegevoegd of verwijderd.

Bij het gebruik van nieuwe digitale systemen of applicaties voeren wij (indien nodig) vooraf een privacytoets of DPIA uit. Zo zorgen we ervoor dat alleen noodzakelijke persoonsgegevens worden verwerkt en dat de beveiliging op orde is.

Werk gerelateerde en contractuele gegevens:
- Opleiding en werkervaring;
- Functie, functietitel, afdeling en datum van indiensttreding;
- Gegevens over het functioneren en prestaties;
- Gegevens over je functie, functietitel en afdeling;
- Gegevens over aan-/afwezigheid;
- Arbeidsovereenkomst (soort contract, begin- en einddatum, contractduur);
- Gegevens over arbeidsvoorwaarden (bijv. afspraken over werktijden, pensioenregeling);
- Gegevens over beëindiging van het dienstverband (bijv. ontslagdatum, redenen voor beëindiging);

Financiële gegevens:
- Salarisinformatie;
- Bankrekeningnummer (accountgegevens).

Belonings- en voordeelgegevens:
- Reiskostenvergoeding;
- Werknemersvoordelen zoals leaseauto, laptop, telefoon;
- Andere secundaire arbeidsvoorwaarden.

Gebruikers- en locatiegegevens;
- Inloggegevens voor onze systemen;
- Locatiegegevens, gebruikersgegevens en km-gegevens (bijv. bij gebruik van een leenauto/dienstauto);
- Gegevens over het netwerkgebruik.

Gegevens in het kader van arbeidsovereenkomst en wetgeving:
- Gegevens die nodig zijn om de arbeidsovereenkomst uit te voeren of aan wettelijke verplichtingen te voldoen.

Gezondheidsgegevens (alleen als dit wettelijk is toegestaan):
- Verzuimregistraties en medische informatie (bij langdurig ziekteverzuim of arbeidsongeschiktheid, via bedrijfsarts);
- Gegevens over aanpassing op de werkplek vanwege gezondheid (bijv. ergonomische maatregelen).

Toegang- en beveiligingsgegevens:
- Camerabeelden voor beveiliging van onze terreinen, objecten en gebouwen;
- Toegang-logs van gebouwen of systemen (bijv. toegangspasgebruik);
- Andere toegangscontrolegegevens.

Een deel van deze gegevens krijgen wij van jou (de medewerker) zelf. Een ander deel van de gegevens ontvangen wij van jouw teammanager/leidinggevende, van de HR-medewerkers en van eventuele externen, denk hierbij bijvoorbeeld aan de Arboarts of een opleidingsinstantie.

Wie verwerken deze persoonsgegevens en waarom?

Afdeling P&O

De afdeling P&O verwerkt jouw persoonsgegevens om de provincie in haar rol als werkgever te ondersteunen. Het gaat hierbij (onder meer) om het opbouwen en bijhouden van het personeelsdossier, het uitvoeren van afspraken uit de arbeidsovereenkomst, de cao en provinciale regelingen, en het uitbetalen van salaris en vergoedingen.

Daarnaast verwerkt deze afdeling persoonsgegevens voor strategische personeelsplanning (SPP). Daarmee wordt gekeken naar de personeelsbehoefte van de provincie in de toekomst, doorgroeimogelijkheden van medewerkers en de ondersteuning van loopbaanontwikkeling

Ook verwerkt de afdeling persoonsgegevens in het kader van verzuimbeleid, verzuimbegeleiding en verzuimpreventie. Dit gebeurt onder meer op grond van de Arbowet en de Wet verbetering poortwachter, zodat medewerkers goed begeleid worden en ziekte waar mogelijk kan worden voorkomen.

Verder worden persoonsgegevens verwerkt voor beleidsontwikkeling, statistiek, onderzoek en

managementinformatie. Waar mogelijk worden gegevens geanonimiseerd of samengevoegd, zodat deze niet naar individuele medewerkers te herleiden zijn.

Tot slot verwerkt de afdeling persoonsgegevens om te voldoen aan wettelijke verplichtingen, zoals het doorgeven van inkomensgegevens aan instanties als de Belastingdienst en het UWV.

Afdeling I&A
De afdeling I&A verwerkt persoonsgegevens om de provincie te ondersteunen bij het beschikbaar stellen van ICT-voorzieningen en het delen van informatie op het gebied van I&A en zakelijke communicatie.

Daarnaast verwerkt I&A persoonsgegevens voor het beheer, onderhoud en de beveiliging van onze digitale werkomgeving (zoals Microsoft 365, Teams, SharePoint en Plein). Daarbij wordt strikt gewerkt volgens de BIO-norm en interne autorisatieprocedures.

Ook kan de afdeling locatiegegevens verwerken om communicatiemiddelen beveiligen. Dit gebeurt alleen met toestemming van de medewerker, bijvoorbeeld om bij verlies van een laptop gegevens op afstand te verwijderen of ontoegankelijk te maken voor derden.

Tot slot verwerkt deze afdeling persoonsgegevens om gegevens te bundelen en te anonimiseren voor beleidsontwikkeling, statistiek,, onderzoek en managementinformatie.

Afdeling FD
De afdeling FD verwerkt persoonsgegevens (onder meer) voor het verstrekken en beschikbaar stellen van facilitaire producten, diensten en voorzieningen, waaronder vervoermiddelen, reserveringen, AV-middelen, werkplekken en vergaderruimtes.

Daarnaast verwerkt de afdeling persoonsgegevens voor het beheer van toegangspassen en de beveiliging van gebouwen en terreinen. Dit omvat onder andere het bewaken van eigendommen en bedrijfsmiddelen en het uitvoeren van parkeerbeleid.

Ook verwerkt de afdeling persoonsgegevens bij het afhandelen van meldingen over verloren of gevonden voorwerpen en bij het oplossen van facilitaire storingen en reparaties binnen de organisatie.

Overige afdelingen verwerken persoonsgegevens voor (onder meer) de volgende doeleinden:

- Het organiseren van verkiezingen in het kader van medezeggenschap (zoals de ondernemingsraad).
- Het doorlopen van accreditatie- en certificeringsprocessen.
- De registratie en opvolging van interne klachten (bijvoorbeeld door de integriteitscoördinator).
- Het nakomen van wettelijke verplichtingen.
- Het ondersteunen bij bedrijfshulpverlening en het verlenen van hulp bij calamiteiten.
- Het bijhouden van rittenregistraties en het beheer van bedrijfsauto's. Hierbij worden bijvoorbeeld namen, contactgegevens, locatiegegevens en kilometerstanden vastgelegd. Deze gegevens worden verzameld bij het gebruik van een leen- of dienstauto en zijn noodzakelijk voor het

afleggen van verantwoording aan de Belastingdienst.
- Voor het privégebruik van leasauto's worden gegevens geregistreerd ten behoeve van de fiscale bijtelling.
- In het kader van privacy en gegevensbescherming: verwerken van contactgegevens van privacy-ambassadeurs en betrokken medewerkers bij DPIA's, datalekmeldingen en bewustwordingsactiviteiten.
- In het kader van Informatiebeveiliging: verwerken van incidentenmanagement (bijv. Topdesk-meldingen).
- In het kader van communicatie, zoals het versturen van interne nieuwsbrieven en uitnodigingen.

Uitzonderlijke omstandigheden waarbij persoonsgegevens worden verwerkt:

In uitzonderlijke situaties kan de provincie toegang krijgen tot je e-mail en/of bestanden. Dit kan bijvoorbeeld als je manager dit nodig heeft om het werk door te laten gaan. Zo'n toegang wordt alleen verleend vai een vaste procedure, met goedkeuring van de CIO en advies van de centrale privacy officers. Hierbij geldt altijd het vierogenprincipe (twee door de CIO aangewezen personen).

Toegang wordt alleen gegeven als contact met jou niet mogelijk is binnen een redelijke termijn, bijvoorbeeld door langdurige ziekte of afwezigheid. Het kan ook nodig zijn om bedrijfscontinuïteit te waarborgen, de veiligheid te bescherming of te voldoen aan een juridische verplichting. Als het kan, word je vooraf geïnformeerd over deze toegang, tenzij dat om juridischeof veiligheidsredenen niet mogelijk is. Toegang en inzage worden (hoofdregel) altijd gelogd en kunnen achteraf worden gecontroleerd door de Functionaris Gegevensbescherming of de centrale privacy officers.

Let op:
Als de aanvraag tot toegang via het CIO-office komt, neemt de directeur Bedrijfsvoering de goedkeuring over. Dit geldt ook bij afwezigheid van de CIO.

Op basis van welke wettelijke AVG-grondslag verzamelen wij (onder meer) jouw persoonsgegevens?

Wij mogen jouw persoonsgegevens alleen verwerken als daar een geldige grondslag voor is. De belangrijkste grondslagen zijn:

- **Uitvoering van de arbeidsovereenkomst**: bijvoorbeeld voor salarisbetaling en verlofregistratie.
- **Wettelijke verplichting**: bijvoorbeeld gegevens die wij moeten doorgeven aan de Belastingdienst, het UWV of bedrijfsarts.
- **Gerechtvaardigd belang**: bijvoorbeeld om veiligheid in onze gebouwen te waarborgen en continuïteit van het werk te garanderen.
- **Toestemming:** in uitzonderlijke gevallen vragen wij je toestemming. Je kunt die altijd weigeren of intrekken.

Met welke derden delen wij jouw persoonsgegevens?

Soms zijn wij wettelijk verplicht om jouw gegevens te delen, bijvoorbeeld met de bedrijfsarts, accountant, de Belastingdienst of het UWV. Ook kunnen wij persoonsgegevens delen met pensioenfondsen, verzekeringsmaatschappijen of opleidingsinstituten, als dat nodig is voor afspraken die we met jou hebben gemaakt.

Daarnaast delen wij soms persoonsgegevens incidenteel met onderzoeks- of adviesbureaus voor interne of externe onderzoeken. Waar mogelijk worden deze gegevens geanonimiseerd of samengevoegd/ gepseudonimiseerd, zodat ze niet meer direct naar jou zijn te herleiden.

Ook maken wij gebruik van software en diensten van externe leveranciers. Met deze leveranciers maken wij duidelijke afspraken in een verwerkersovereenkomst over de bescherming van jouw persoonsgegevens. We werken bij voorkeur met partijen die gevestigd zijn binnen de Europese Economische Ruimte (EER). Als gegevens toch buiten de EER worden verwerkt, zorgen we voor passende waarborgen, zoals de modelcontracten van de Europese Commissie of aanvullende beveiligingsmaatregelen.

Hoe lang bewaren wij jouw persoonsgegevens?

Wij bewaren jouw persoonsgegevens niet langer dan nodig is voor het doel waarvoor ze zijn verzameld. Hoe lang dit precies is, verschilt per soort informatie.

De afdeling DIV bewaakt de bewaartermijnen op basis van de Archiefwet en de geldende selectielijst (d.d. 1 januari 2020). Een deel van de gegevens wordt ook bewaard nadat je uit dienst bent, bijvoorbeeld voor fiscale of wettelijke verplichtingen.

De algemene bewaartermijn is twee jaar, tenzij wetgeving of de selectielijst een langere termijn voorschrijft.

Hoe beschermen wij jouw persoonsgegevens?

Binnen de provincie maken wij gebruik van beveiligingssystemen en standaarden om jouw persoonsgegevens te beschermen. Deze worden regelmatig bijgewerkt om te blijven voldoen aan nieuwe wetgeving, beleidskaders en technologische ontwikkelingen.

Naast technische maatregelen, zoals het versleutelen van gegevens en het toepassen van toegangscontroles, geldt voor medewerkers ook een wettelijke geheimhoudingsplicht (artikel 9 Ambtenarenwet en de afgelegde ambtseed). Toegang tot persoonsgegevens wordt alleen verleend aan medewerkers die daar bevoegd toe zijn. Bij het bepalen van beveiligingsmaatregelen houden we rekening met de stand van de techniek en passen we deze waar nodig aan.

De provincie werkt volgens de **Baseline Informatiebeveiliging Overheid (BIO)**. Waar relevant bereiden wij ons ook voor op de verplichtingen uit de **NIS2-richtlijn**. Daarnaast investeren we in bewustwording: medewerkers ontvangen regelmatig trainingen en nieuwsberichten over privacy, veilig werken en informatiebeveiliging.

Je kunt zelf ook bijdragen aan de bescherming van jouw gegevens en die van anderen. Denk daarbij aan:

- je laptop te vergrendelen als je je werkplek verlaat;
- een sterk wachtwoord te gebruiken;
- je inloggegevens niet te delen met anderen;
- vertrouwelijke documenten beveiligd op te slaan;

- zorgvuldig om te gaan met gevoelige informatie in vergaderingen of telefoongesprekken (regel zo nodig een afgesloten ruimte);
- alleen te werken in beveiligde systemen en geen persoonsgegevens te versturen via privé-mail of apps;
- alert te zijn op phishing en verdachte links of bijlagen niet te openen, bij het opmerken een melding hiervan maken;
- geen persoonsgegevens in te voeren in (openbare) AI-tools.

Wie houden zich binnen de organisatie bezig met de AVG?

Functionaris Gegevensbescherming (FG)
De provincie Gelderland heeft een Functionaris Gegevensbescherming (FG) aangesteld. De FG ziet erop toe dat de provincie de privacywetgeving naleeft en doet dat onafhankelijk. De FG rapporteert rechtstreeks aan de directie, en brengt ook adviezen en bevindingen in bij het CMT en AMT. Zo wordt geborgd dat de hoogste leiding en het management tijdig zicht hebben op risico's en verbeterpunten.

Verder controleert de FG onder andere of persoonsgegevens juist en zorgvuldig worden verwerkt en of passende maatregelen zijn getroffen om deze te beschermen.

Privacy Officer centraal (PO)
De Centrale Privacy Officers (PO's) werken vanuit het CIO-office. Zij zijn de privacy-experts van de provincie. Hun taak is om ervoor te zorgen dat de provincie in de praktijk goed met de AVG en privacyregels omgaat. Anders dan de FG zijn de PO's verantwoordelijk voor de dagelijkse uitvoering van het privacybeleid. De taken van de PO's zijn bijvoorbeeld:

- het opstellen en bijhouden van het privacybeleid, het verwerkingsregister en het datalekprotocol;
- het helpen van projectleiders bij het uitvoeren van een Data Protection Impact Assessment (DPIA), waarmee privacyrisico's van een project in kaart worden gebracht;
- het adviseren over de noodzaak en het beoordelen van een verwerkersovereenkomst, gegevensleveringsovereenkomst of samenwerkingsovereenkomst waarbij persoonsgegevens worden gedeeld;
- het geven van advies over de naleving van de AVG en het ondersteunen van medewerkers bij vragen of knelpunten;
- het begeleiden van datalekken en, indien nodig, de melding daarvan aan de Autoriteit Persoonsgegevens;
- het organiseren en geven van kennissessies, trainingen en workshops over privacy aan teams, afdelingen, het CMT en AMT;
- het signaleren van nieuwe wetgeving of ontwikkelingen inzake persoonsgegevens en het vertalen daarvan naar de praktijk binnen de provincie.

De PO's stemmen hun werkzaamheden indien nodig af met de Chief Information Security Officer (CISO) en de data-officers binnen het CIO-office, zodat privacy, informatiebeveiliging en datakwaliteit samenhangend worden geborgd.

Om dit goed te doen, zijn de PO's afhankelijk van de informatie die zij krijgen uit de organisatie: van de medewerkers, maar vooral van de privacy-ambassadeurs die op de afdelingen werken.

Privacy Ambassadeur van jouw afdeling
De Privacyambassadeur (PA) is het eerste aanspreekpunt voor privacy op jouw afdeling. Hij of zij beantwoordt eenvoudige vragen en helpt collega's op weg bij het zorgvuldig omgaan met persoonsgegevens.

Daarnaast heeft de PA een signalerende rol: risico's binnen de afdeling, samenwerkingen waarbij persoonsgegevens gedeeld worden, of complexe privacyvraagstukken worden (waar nodig) doorgezet naar de centrale Privacy Officers (PO's).

De PA helpt de afdeling om volgens het privacybeleid te werken. Als blijkt dat er onvoldoende bewustzijn is bij collega's, schakelt de PA de PO's in voor advies, kennissessies of trainingen.

Zo zorgen we samen voor een goed werkende privacyorganisatie, waarin ieder (vanuit zijn of haar eigen rol) bijdraagt aan een zorgvuldige en veilige omgang met persoonsgegevens.

Jouw rechten

Je hebt de volgende rechten ten opzichte van de verwerking van jouw persoonsgegevens door de provincie Gelderland:

- Recht op inzage: Je hebt het recht om te weten welke persoonsgegevens wij van jou verwerken.
- Recht op informatie: Je hebt recht op duidelijk uitleg over waarom en op welke manier wij jouw persoonsgegevens verwerken.
- Recht op correctie: Je kunt vragen om onjuiste of onvolledige persoonsgegevens te corrigeren of aan te vullen.
- Recht op verwijdering: Je kunt verzoeken om jouw persoonsgegevens te verwijderen, bijvoorbeeld wanneer ze niet langer nodig zijn.
- Recht op beperking van verwerking: Je kunt vragen om de verwerking van jouw persoonsgegevens tijdelijk of gedeeltelijk te beperken, bijvoorbeeld tijdens een onderzoek naar de juistheid ervan.
- Recht van bezwaar: Je kunt bezwaar maken tegen de verwerking van jouw persoonsgegevens wanneer je bijvoorbeeld uitnodigingen voor evenementen per post ontvangt en jij dit niet op prijs stelt.
- Recht op overdraagbaarheid: Je kunt ons verzoeken om jouw persoonsgegevens in een gestructureerde, gangbare en leesbare vorm aan jou of een andere organisatie over te dragen.
- Recht van bezwaar tegen geautomatiseerde besluitvorming: Je kunt bezwaar maken tegen besluiten die uitsluitend gebaseerd zijn op geautomatiseerde verwerking, wanneer deze juridische gevolgen hebben of jou anderszins significant treffen.

Let op: deze rechten gelden niet altijd en overal. Soms zijn wij wettelijk verplicht om bepaalde gegevens te bewaren of hebben wij ze nog nodig om ons werk goed te kunnen doen. Als wij je verzoek (gedeeltelijk) niet kunnen uitvoeren, leggen we altijd uit waarom.

Hoe dien je een verzoek in?
Je kunt een verzoek indienen voor het uitoefenen van jouw rechten via het knopje 'Privacy & AVG' op het plein. Jouw verzoek wordt in beginsel binnen vier weken afgehandeld. In sommige gevallen, bijvoorbeeld wanneer jouw verzoek complex is of meerdere gegevens omvat, kan deze termijn worden verlengd tot maximaal twee maanden. Als dit zo is, ontvang je hier een uitleg van.

Hoe specifieker je bent bij de aanvraag, hoe sneller wij jouw verzoek kunnen behandelen. Probeer daarom duidelijk aan te geven op welke gegevens of verwerkingen jouw verzoek betrekking heeft. Dit helpt ons om efficiënt de juiste informatie te verzamelen en jou snel van een reactie te voorzien.

Let op: Hoewel wij ons inspannen om aan ieder verzoek te voldoen, kunnen technische beperkingen of beperkingen binnen onze systemen ervoor zorgen dat bepaalde gegevens moeilijk te vinden of te verwijderen zijn. In zulke gevallen zullen wij ons uiterste best doen om alternatieve oplossingen te bieden en je hierover goed te informeren.

Datalek melden

Een datalek betekent dat er iets misgaat met de beveiliging van persoonsgegevens. Daardoor worden de gegevens per ongeluk of op een verkeerde manier verwerkt.

Dit kan gebeuren als gegevens verloren gaan, vernietigd worden, gewijzigd raken, onbevoegd toegankelijk zijn of ongeoorloofd openbaar worden gemaakt.

Voorbeelden van een datalek:

- Verkeerd geadresseerde e-mails: Persoonsgegevens of vertrouwelijke documenten worden per ongeluk naar de verkeerde ontvanger gestuurd, zowel intern als extern. Dit is een van de meest voorkomende datalekken.
- Verlies of diefstal van laptops, mobiele telefoons of tablets: Onbeveiligde apparaten met toegang tot systemen en gegevens raken kwijt of worden gestolen, bijvoorbeeld onderweg of op kantoor.
- Onjuist gedeelde bestanden op SharePoint of Teams: Vertrouwelijke bestanden worden verkeerd geconfigureerd of gedeeld met personen die geen toegang zouden moeten hebben, bijvoorbeeld doordat rechten verkeerd zijn ingesteld.
- Openbare printers met achtergelaten documenten: Gevoelige documenten, zoals personeelsgegevens of contracten, blijven onbeheerd achter op printers in gedeelde ruimtes.
- Onbeveiligde fysieke dossiers: Papieren dossiers met persoonsgegevens worden niet goed opgeborgen (bijvoorbeeld in ongecontroleerde archiefruimtes) of worden achtergelaten op bureaus.
- Verlies van toegangskaarten met gevoelige toegangsinformatie: Medewerkers verliezen hun toegangspas, wat kan leiden tot onbevoegde toegang tot fysieke locaties en mogelijk gegevens.
- Gegevens lekken via onbeveiligde e-mails of niet-versleutelde communicatie: Vertrouwelijke informatie wordt verstuurd zonder versleuteling, waardoor het onderweg onderschept kan worden.
- Fouten bij verwerking van persoonsgegevens in systemen: Onjuiste invoer van gegevens of een foutieve koppeling tussen systemen kan leiden tot verkeerde verwerking of het per ongeluk beschikbaar stellen van gegevens.
- Onbeveiligde werkplekken: Medewerkers vergrendelen hun werkplek niet wanneer ze hun bureau verlaten, waardoor collega's of onbevoegden toegang kunnen krijgen tot gevoelige informatie.
- Onjuiste opslag of verwijdering van bestanden: Bestanden met persoonsgegevens worden niet op de juiste plaats opgeslagen of blijven onnodig lang in systemen staan, zonder tijdige verwijdering volgens de bewaartermijnen.

Waarom is een datalek zo belangrijk om te melden?

Een datalek kan grote gevolgen hebben voor de mensen van wie de gegevens zijn gelekt: denk aan identiteitsfraude of reputatieschade. Ook voor de organisatie zelf kunnen de gevolgen groot zijn. Daarom nemen we datalekken serieus.

Meldplicht bij de Autoriteit Persoonsgegevens
Als een datalek risico's oplevert voor de privacy van betrokkenen, zijn we wettelijk verplicht om dit binnen 72 uur te melden bij de Autoriteit Persoonsgegevens (AP).

Deze meldplicht geldt niet als duidelijk is dat het risico voor betrokkenen verwaarloosbaar is. In sommige gevallen moeten we ook de betrokken personen zelf informeren, bijvoorbeeld als er een hoog risico is op identiteitsfraude of financiële schade. Of er een meldplicht geldt, beoordelen de privacy officers (soms samen met de FG) op basis van de situatie.

Wat moet je doen bij een vermoeden van een datalek?
Als je denkt dat er sprake is van een datalek, meld dit dan zo snel mogelijk (binnen 24 uur) via het plein **Melding vermoeden datalek - Selfserviceportal (prvgld.nl)** . Hoe eerder een datalek wordt gemeld, hoe sneller de privacy officers kunnen beoordelen of verdere maatregelen nodig zijn om schade te beperken en aan de meldplicht te voldoen.

Welke informatie moet je bij de melding geven?
Bij het melden van een datalek is het belangrijk om de volgende informatie zo snel en volledig mogelijk aan te leveren. Denk aan vragen zoals:

- Wat is er gebeurd?
- Welke (soort) gegevens zijn betrokken?
- Wie is erbij betrokken?
- Is je leidinggevende al op de hoogte?
- Welke maatregelen zijn al genomen?

Hoe volledi ger je melding, hoe beter de privacy officers kunnen beoordelen wat er moet gebeuren.

Veilig mailen

Wanneer je persoonsgegevens of andere vertrouwelijke informatie deelt met externe partijen (zoals burgers, bedrijven of samenwerkingspartners), moet dat op een **veilige manier** gebeuren.
Gebruik daarom altijd de beveiligde mailvoorziening die de provincie daarvoor beschikbaar stelt. Welke middelen dit zijn, vind je op het Plein onder **'Veilig mailen'**.

De privacy officers zien dat veel datalekken ontstaan doordat gevoelige informatie per ongeluk naar de verkeerde persoon wordt gemaild of zonder versleuteling wordt verstuurd. Door gebruik te maken van een beveiligde mailvoorziening voorkom je dit soort fouten en voldoe je aan de **AVG-verplichting** om persoonsgegevens op een passende manier te beveiligen.

Meer informatie, handleidingen en het actuele overzicht van beschikbare middelen vind je op het Plein.

Klacht indienen

Heb je een klacht over hoe wij omgaan met jouw persoonsgegevens? Dan kun je dit melden via de Privacy Ambassadeur van jouw afdeling, via de privacy officers (privacy@gelderland.nl) of via de FG (fg@gelderland.nl).

Wanneer je vervolgens nog steeds niet tevreden bent over de afhandeling van je klacht, kun je een klacht indienen bij de Autoriteit Persoonsgegevens via https://www.autoriteitpersoonsgegevens.nl

Wijzigingen in deze privacyverklaring

Onze privacyverklaring kan worden aangepast wanneer er wijzigingen zijn in de wet of in de manier waarop wij jouw gegevens verwerken. We vinden het belangrijk dat jij altijd op de hoogte ben van deze wijzigingen. Bij substantiële wijzigingen zullen wij dan ook tijdig een bericht op de binnenplaats hierover plaatsen en indien nodig instemming van de OR vragen. De meest recente versie is altijd beschikbaar op onze Sharepointpagina en op het Plein.