WAG &
PARTNERS
- Registeraccountants -

Privacybeleid

Dit betreft versie 2025.1

Inhoudsopgave

1 Inleiding

WAG & Partners B.V. (hierna 'WAG') verwerkt als accountantsorganisatie persoonsgegevens. WAG beschikt en verwerkt iedere dag gegevens van klanten en medewerkers en overige betrokkenen. Het is van het grootste belang dat zorgvuldig met deze informatie wordt omgegaan en dat de privacy van alle betrokkenen gewaarborgd blijft. Het respecteren en beschermen van de privacy en persoonsgegevens van de klant maakt ook onlosmakelijk onderdeel uit van de kwaliteit van de dienstverlening. Naast het leveren van zijn dienstverlening dient WAG ook zorg te dragen voor de privacy van zijn medewerkers en alle andere betrokkenen.

Dit beleid heeft betrekking op de bescherming van persoonsgegevens van alle betrokkenen bij WAG. Het gaat hier in ieder geval om persoonsgegevens van alle medewerkers, klanten, bezoekers en externe relaties, ongeacht of het in een systeem zit of in een persoonlijk notitieboek.

Om ervoor te zorgen dat WAG voldoet aan de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) en de Uitvoeringswet AVG, is het van belang dat alle medewerkers op de hoogte zijn van dit privacybeleid. Het privacybeleid geeft aan hoe elke medewerker veilig met persoonsgegevens om dient te gaan. Uiteindelijk is elke medewerker verantwoordelijk voor een juiste omgang met persoonsgegevens. Voor vragen en extra informatie kunnen medewerkers contact opnemen met de compliance officer.

1.1 Doelstelling

Het doel van dit privacybeleid is om de kwaliteit van de gegevensverwerking te optimaliseren, waarbij rekening wordt gehouden met een goede balans tussen privacy, functionaliteit en veiligheid. Dit beleid wordt vertaald in procedures en richtlijnen aansluitend op de aard van de verwerkingen binnen de verschillende soorten processen.

1.2 Borging van dit beleid

WAG maakt gebruik van de Plan-Do-Check-Act cyclus (PDCA) bij het borgen van het beleid. De compliance officer beheert en actualiseert het beleid. Het bestuur evalueert jaarlijks het beleid.

2 Definities

In dit beleid wordt het volgende begrippenkader gehanteerd:

Afkorting/definitie	Toelichting
Autoriteit Persoonsgegevens (AP)	De toezichthouder die tot taak heeft toe te zien op de verwerking van persoonlijke gegevens conform de AVG.
AVG	Algemene Verordening Gegevensbescherming.
Beveiliging	Het samenhangend stelsel van passende technische en organisatorische maatregelen om gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.
Beveiligingsincident	Een gebeurtenis *waarbij de mogelijkheid bestaat* dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of kan komen.

Bestand	Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
Betrokkene	Natuurlijk persoon op wie een persoonsgegeven betrekking heeft.
Bijzondere persoonsgegevens	Persoonsgegevens die in beginsel verboden zijn om te verwerken. Het gaat om verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.
Datalek	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
Derde	Niet zijnde de betrokkene, de verantwoordelijke, de verwerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de verwerker gemachtigd is om persoonsgegevens te verwerken.
Functionaris Gegevensbescherming (FG)	De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de AVG binnen WAG.
Gevoelige persoonsgegevens	Persoonsgegevens die gelet op de inhoud of naar hun aard als gevoelig worden aangemerkt, omdat dit bijvoorbeeld iets zegt over iemands gedrag of financiële situatie, het een kwetsbare groep (zoals kinderen) betreft of bijvoorbeeld het burgerservicenummer (BSN).
Identificeerbare gegevens	Gegevens die zonder onevenredige tijd en moeite aan de betrokkene zijn te koppelen.
Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
Verwerkingsverantwoordelijke	De organisatie die het doel en de middelen voor de gegevensverwerking bepaalt.
Verstrekken van persoonsgegevens	Het bekend maken of ter beschikking stellen van gegevens.
Verwerker	Een organisatie die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
Verwerking van persoonsgegevens	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling,

	samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Verzamelen van persoonsgegevens	Het verkrijgen/ontvangen van persoonsgegevens.

3 Beginselen en rechtmatigheid

Alle verwerkingsactiviteiten en bijbehorende persoonsgegevens die worden uitgevoerd door, binnen of namens WAG moeten voldoen aan de beginselen uit de AVG. Dit verwezenlijken wij op de volgende manier.

Rechtmatigheid, behoorlijkheid en transparantie

WAG verwerkt persoonsgegevens volgens de beginselen uit de AVG. Alle verwerkingen binnen, door of namens de organisatie moeten rechtmatig, behoorlijk en transparant zijn. Dit betekent dat betrokkene geïnformeerd moet zijn over de verwerking en dat deze in overeenstemming met de wet plaatsvindt.

Doelbinding

Doelbinding houdt in dat persoonsgegevens alleen worden verzameld voor specifieke, gerechtvaardigde doelen, zoals werkgeverschap, dienstverlening, contractsluiting of interne bedrijfsvoering. Elk ander gebruik moet vooraf worden afgestemd met de compliance officer.

Minimale gegevensverwerking

Minimale gegevensverwerking betekent dat alleen noodzakelijke persoonsgegevens worden verwerkt. Persoonsgegevens die niet noodzakelijk zijn voor het doel mogen in beginsel niet verzameld worden. Medewerkers beoordelen of gegevens relevant zijn en of anonimiseren mogelijk is. Denk hierbij o.a. aan tekststukken zwart maken, namen omzetten naar nummers, kolommen verwijderen uit Excel spreadsheets. Toegang tot persoonsgegevens is beperkt tot wat nodig is.

Juistheid

Juistheid vereist dat gegevens correct zijn. Onjuiste informatie moet worden gecorrigeerd of verwijderd zodra dit geconstateerd wordt.

Opslagbeperking

Opslagbeperking houdt in dat gegevens niet langer bewaard worden dan noodzakelijk, conform het **Data retentiebeleid** van WAG.

Integriteit en vertrouwelijkheid

Integriteit en vertrouwelijkheid worden gewaarborgd door passende technische en organisatorische maatregelen om gegevens te beschermen tegen verlies, schade of onbevoegde toegang.

Verantwoordingsplicht

Verantwoordingsplicht betekent dat WAG de naleving van deze principes moet kunnen aantonen via beleid, registers, verwerkersovereenkomsten, toezicht door de compliance officer en andere waarborgen zoals privacy by design/default. Indien WAG zijn verplichtingen niet of onvoldoende nakomt, kan hij aansprakelijk gesteld worden door betrokkenen en eventuele maatregelen en/of boetes opgelegd krijgen vanuit de Autoriteit Persoonsgegevens.

Rechtmatigheid

Rechtmatigheid van gegevensverwerking is een basisprincipe uit de AVG. WAG moet voor elke verwerking een geldige wettelijke grondslag kunnen aantonen. WAG dient elke verwerking te baseren op één van de volgende gronden:

- **Toestemming** is alleen geldig als deze specifiek, geïnformeerd, vrijwillig en actief is gegeven. Werknemers kunnen vaak geen volledig vrije toestemming geven vanwege de gezagsverhouding.

- **Uitvoering van een overeenkomst** is een veelgebruikte grondslag, bijvoorbeeld bij arbeidscontracten of dienstverlening aan klanten. De verwerking moet noodzakelijk zijn voor de uitvoering van de overeenkomst.
- **Wettelijke verplichting** geldt wanneer verwerking verplicht is volgens wet- en regelgeving, zoals de Wwft of fiscale wetten.
- **Vitale belangen** zijn zelden van toepassing, maar kunnen gelden in noodgevallen, bijvoorbeeld bij medische incidenten. Bijvoorbeeld wanneer iemand bewusteloos is en geen toestemming kan geven om zijn persoonsgegevens te verwerken.
- **Taak van algemeen belang** is alleen van toepassing indien de persoonsgegevens daadwerkelijk noodzakelijk zijn voor de verwerking in verband met de uitoefening van een publiekrechtelijke taak. WAG kan geen beroep doen op deze grondslag.
- **Gerechtvaardigd belang** kan een grondslag zijn als er een evenwicht is tussen het belang van WAG en de privacy van de betrokkene. Proportionaliteit en subsidiariteit moeten worden gewaarborgd en de afweging moet gedocumenteerd zijn.

Bijzondere persoonsgegevens

Het is belangrijk dat opgemerkt wordt dat persoonsgegevens in verschillende categorieën vallen. De hierboven beschreven voorwaarden voor rechtmatigheid zijn op het grootste deel van persoonsgegevens van toepassing. Echter is een aantal categorieën persoonsgegevens uitgezonderd.

Artikel 9 (1) AVG bepaalt dat de verwerking van de volgende persoonsgegevens in beginsel verboden is[1]:

- Persoonsgegevens waaruit ras of etnische afkomst blijken;
- Persoonsgegevens waaruit politieke, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken;
- Verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon;
- Gegevens over gezondheid (medische gegevens) of met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Deze categorieën persoonsgegevens zijn bijzonder gevoelig. Deze categorieën persoonsgegevens hebben extra bescherming nodig, omdat het bekend worden van deze gegevens mogelijk negatieve gevolgen voor de betrokkene kan hebben.

Bijzondere persoonsgegevens mogen in principe niet verwerkt worden, tenzij een uitzondering geldt. Professionals die hiermee te maken krijgen, moeten altijd vooraf overleggen met de compliance officer.

[1] Bijzondere persoonsgegevens mogen alleen bij uitzondering worden verwerkt. De uitzondering worden benoemd in artikel 9 lid 2 AVG en de artikelen 22 tot en met 30 UAVG.

4 Governance

4.1 Risk appitite WAG

Het bestuur van WAG bepaalt, op basis van een risicoanalyse, welke risico's het bereid is te accepteren bij het nastreven van de strategische doelstellingen. Deze risicobereidheid, ook wel 'risk appetite' genoemd, geeft aan binnen welke grenzen WAG opereert. Vallen risico's buiten deze grenzen, dan zijn extra beheersmaatregelen nodig.

Voor privacy geldt, op basis van de SIRA-methodiek, een 'Gemiddeld' bruto risico. Dit niveau is ook vastgesteld als de risk appetite voor privacy. In **bijlage I** zijn de relevante scenario's en berekeningen verder uitgewerkt.

4.2 Taken en verantwoordelijkheden

4.2.1 Bestuur en kwaliteitsbepaler

Het bestuur is eindverantwoordelijk voor het privacybeleid. Eén bestuurslid treedt op als kwaliteitsbepaler en is belast met:

- het vaststellen en bijwerken van het privacybeleid;
- het toezien op een correcte naleving van de AVG binnen de organisatie;
- het periodiek evalueren van de effectiviteit van het beleid en bijsturen waar nodig.

4.2.2 Compliance officer

De compliance officer ondersteunt het bestuur en de medewerkers bij het uitvoeren van het privacybeleid en is het eerste aanspreekpunt voor privacyvragen. De taken van de compliance officer zijn onder andere:

- volgen van ontwikkelingen in wet- en regelgeving (AVG);
- adviseren over de impact van deze ontwikkelingen op de organisatie;
- helpen bij het opstellen en uitvoeren van procedures zoals risicoanalyses;
- zorgen voor bewustwording en kennisdeling over privacy binnen het kantoor;
- toezicht houden op dataverwerkingen en de naleving van het beleid;
- afhandelen van verzoeken van betrokkenen.

De compliance officer rapporteert rechtstreeks aan het bestuur.

4.2.3 Medewerkers

Alle medewerkers zijn verantwoordelijk voor het naleven van het privacybeleid in hun dagelijkse werkzaamheden. Het bestuur ziet erop toe dat medewerkers dit beleid begrijpen en correct toepassen.

4.3 Plan-Do-Check-Act

Ons kantoor past de Plan-Do-Check-Act (PDCA)-cyclus toe om het privacybeleid en de bijbehorende procedures actueel, effectief en werkbaar te houden. Deze werkwijze helpt bij het uitvoeren, controleren en verbeteren van het beleid. Zie ook **bijlage II**, waarin dit visueel is weergegeven.

Privacy wordt benaderd op basis van risico's. Jaarlijks voert de Privacy Officer een risicoanalyse uit. Op basis hiervan worden, in overleg met de organisatie, passende maatregelen vastgesteld en ingevoerd. Daarna wordt gecontroleerd of deze maatregelen goed werken en of het beleid nog aansluit bij de praktijk.

Als blijkt dat iets niet effectief is of verouderd, worden aanpassingen gedaan. Dit gebeurt in samenwerking tussen de Privacy Officer en het bestuur of de leiding van het kantoor.

5 Hoofddoelen verwerking binnen WAG

WAG verwerkt persoonsgegevens in verschillende situaties. Het gaat vooral om gegevens van medewerkers, klanten, sollicitanten, leveranciers en bezoekers. Hieronder lichten we de hoofddoelen en bijbehorende categorieën gegevens toe. Meer details zijn opgenomen in onze privacyverklaring.

5.1 Medewerkers

Wij verwerken persoonsgegevens van medewerkers voor de volgende doelen:

Doel	**Categorieën persoonsgegevens**
Aangaan en uitvoeren van arbeidsovereenkomsten	Naam, adres, contactgegevens, financiële en ID-gegevens, prestatie- en verzuimgegevens, familiegegevens, assessmentresultaten
Persoonlijke ontwikkeling	Opleidings-, loopbaan- en beoordelingsgegevens
Interne ondersteuning	Gegevens via IT-middelen (zoals laptops en telefoons)
Voldoen aan wettelijke verplichtingen	Bijv. kopie ID voor loonadministratie
Noodgevallen	Contactgegevens van familieleden
Bedrijfsvoering en systeembeveiliging	Aanwezigheids- en urengegevens, personeelsnummer, IP-adres

Elke medewerker ontvangt de privacyverklaring bij indiensttreding.

5.2 Klanten

Van klanten verwerken wij persoonsgegevens voor:

Doel	**Categorieën persoonsgegevens**
Klantacceptatie	Contact- en bedrijfsgegevens, gegevens over UBO’s
Uitvoering van opdrachten	Afhankelijk van de opdracht o.a. gegevens van medewerkers en klanten van de klant, mogelijk ook bijzondere persoonsgegevens

Doel	Categorieën persoonsgegevens
Klantadministratie	Contact- en bedrijfsgegevens
Bedrijfsvoering	Contact-, betalings- en bedrijfsgegevens
Relatiebeheer & marketing	Contact- en bedrijfsgegevens

5.3 Overige betrokkenen

Ook van andere betrokkenen verwerken wij gegevens:

Groep	Doel	Categorieën persoonsgegevens
Sollicitanten	Werving nieuw personeel	Sollicitatie- en contactgegevens
Leveranciers	Overeenkomsten sluiten	Contact-, betalings- en bedrijfsgegevens
Bezoekers kantoor	Bezoekersregistratie	Naam, bedrijfsnaam, kenteken
Websitebezoekers	Informatieverstrekking en analyse	Contactgegevens, cookies

6 Privacymanagement

Een belangrijk onderdeel van de AVG is de verantwoordingsplicht: het kunnen aantonen dat je zorgvuldig met persoonsgegevens omgaat. Ook voor een kleiner kantoor is het belangrijk om privacy structureel te borgen. Hieronder lees je hoe wij dat doen.

6.1 Bewustwording (Awareness)

Medewerkers spelen een centrale rol in de bescherming van persoonsgegevens. Daarom zorgen we voor regelmatige aandacht voor privacy, onder andere via:

- informatie bij indiensttreding;
- periodieke training;
- praktische hulpmiddelen zoals handleidingen.

Het bestuur geeft hierin het goede voorbeeld en grijpt in als medewerkers zich niet aan het beleid houden.

6.2 Verwerkingsregister

We houden een overzicht bij van alle manieren waarop we persoonsgegevens verwerken: het verwerkingsregister. Hierin staan per activiteit o.a. het doel, de soort gegevens, de betrokken personen, de ontvangers en de bewaartermijnen. Dit register helpt om inzicht te houden in onze verwerkingen en vormt de basis voor risicobeoordeling.

De compliance officer beheert het register en gebruikt input uit de verschillende onderdelen van het kantoor. Verwerkingen in de dienstverlening worden gekoppeld aan onze producten en diensten.

6.3 Risico's en maatregelen

Wij hanteren een risicogerichte aanpak: hoe groter het risico, hoe zwaarder de beheersmaatregelen. Voor elke verwerking beoordelen we het risicoprofiel. Op basis daarvan worden passende maatregelen genomen, vastgelegd door de compliance officer.

DPIA (Data Protection Impact Assessment): Bij verwerkingen met verhoogd risico voeren we een DPIA uit, zoals voorgeschreven door de Autoriteit Persoonsgegevens.

Informatiebeveiliging: We beschermen gegevens met passende technische en organisatorische maatregelen. Hoe gevoeliger de gegevens, hoe strenger de beveiliging.

Privacy by design: Bij nieuwe systemen of diensten houden we vanaf het begin rekening met privacy. Zonder dit aspect wordt een voorstel niet goedgekeurd.

Actualisatie: Bij wijzigingen in systemen of processen evalueren we opnieuw de risico's en passen we de maatregelen aan waar nodig.

6.4 Verwerkers en overeenkomsten

Als wij externe partijen inschakelen die namens ons persoonsgegevens verwerken (zoals IT-leveranciers), sluiten wij altijd een verwerkersovereenkomst. Hierin staan afspraken over beveiliging, geheimhouding en naleving van de AVG.

Alle verwerkers worden zorgvuldig geselecteerd en periodiek gecontroleerd. Alleen als een wettelijke verplichting dit voorschrijft, delen we gegevens met anderen die deze op eigen titel verwerken.

6.5 Rol WAG richting klanten

Organisaties die persoonsgegevens verwerken, kunnen dit doen in de hoedanigheid van '**verwerkingsverantwoordelijke'** of als '**verwerker'**.

- **Verwerkingsverantwoordelijke**: bepaalt het doel en de middelen van de verwerking.
- **Verwerker**: voert de verwerking uit in opdracht van een verwerkingsverantwoordelijke, volgens diens instructies.
- **Gezamenlijke verantwoordelijkheid**: wanneer beide partijen samen bepalen wat er met de gegevens gebeurt.

Wij volgen hierbij de richtlijnen van de beroepsorganisaties binnen onze sector. Deze zijn opgesteld om duidelijkheid te geven over de AVG-rolverdeling bij verschillende soorten opdrachten.

6.5.1 Onze rol per soort opdracht

Type opdracht	**Rol klant**	**Onze rol**
Controle van de jaarrekening (Standaarden 100–999)	Verwerkingsverantwoordelijke	Verwerkingsverantwoordelijke
Beoordelingsopdrachten (Standaarden 2000–2699)	Verwerkingsverantwoordelijke	Verwerkingsverantwoordelijke
Assurance-opdrachten, geen historische cijfers (Standaarden 3000–3850)	Verwerkingsverantwoordelijke	Verwerkingsverantwoordelijke
Rapport van feitelijke bevindingen (Standaard 4400)	Verwerkingsverantwoordelijke	Verwerker* of verwerkingsverantwoordelijke**
Samenstellingsopdrachten (Standaard 4410)	Verwerkingsverantwoordelijke	Verwerkingsverantwoordelijke
Adviesdiensten (geen standaard)	Verwerkingsverantwoordelijke	Verwerkingsverantwoordelijke (indien verwerking van persoonsgegevens geen primair doel is)

* Als de opdracht direct gericht is op het verwerken van persoonsgegevens.
** Als de verwerking slechts een neveneffect is van de opdracht.

6.5.2 Praktische toepassing

Bij elke opdracht bekijken we of we zelf beslissen over het gebruik van persoonsgegevens of dat we uitsluitend werken op instructie van de klant. In het eerste geval zijn wij verwerkingsverantwoordelijke; in het tweede geval verwerker. Dit is belangrijk om vast te stellen, omdat dit invloed heeft op onze verplichtingen en welke afspraken we met de klant moeten vastleggen.

Wanneer wij als verwerker optreden, zorgen we ervoor dat er een verwerkersovereenkomst wordt gesloten (opgenomen in de algemene voorwaarden), waarin afspraken staan over beveiliging, geheimhouding en verantwoordelijkheden.

6.6 Rechten van betrokkenen

Iedereen van wie wij persoonsgegevens verwerken – ook wel "betrokkenen" genoemd – heeft rechten op basis van de AVG. Denk hierbij aan het recht op inzage, correctie, verwijdering of het overdragen van gegevens

(dataportabiliteit). Een betrokkene hoeft geen reden op te geven en mag op elk moment vragen welke gegevens van hem of haar zijn vastgelegd.

Om misbruik te voorkomen, vragen we altijd om een geldig identiteitsbewijs voordat we een verzoek in behandeling nemen. Zonder identificatie kunnen we het verzoek niet verwerken. Wij reageren binnen één maand op elk geldig verzoek.

Wanneer wij als verwerkingsverantwoordelijke optreden (bijvoorbeeld voor onze eigen medewerkers of klanten), behandelen wij het verzoek zelf. Als wij slechts als verwerker optreden (bijvoorbeeld namens een klant), sturen we het verzoek door naar de klant, die dan bepaalt wat ermee gebeurt.

6.6.1 Uitzonderingen

In een aantal gevallen mag een verzoek worden geweigerd. De AVG geeft hiervoor de volgende uitzonderingen:

1. nationale veiligheid
2. landsverdediging
3. de openbare veiligheid
4. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid
5. andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid
6. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures
7. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen
8. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten 1, tot en met 5 en punt 7 bedoelde gevallen
9. de bescherming van de betrokkene of van de rechten en vrijheden van anderen
10. de inning van civielrechtelijke vorderingen

In ons geval zijn vooral de uitzonderingen rond beroepsregels, toezicht en bescherming van derden relevant. De compliance officer beoordeelt of zo'n uitzondering van toepassing is.

6.6.2 Bezwaar maken

Als WAG persoonsgegevens verwerken op basis van een gerechtvaardigd belang (van onszelf of een derde), mag de betrokkene daar bezwaar tegen maken. Wij stoppen dan met verwerken, tenzij we zwaarder wegende belangen kunnen aantonen. Bij direct marketing stoppen we altijd direct met de verwerking als iemand bezwaar maakt.

Wij nemen geen besluiten die volledig geautomatiseerd tot individuele gevolgen leiden (zoals profilering). Mochten we dit in de toekomst wel doen, dan zorgen we voor menselijke tussenkomst, zoals de AVG voorschrijft.

6.6.3 Klachten

Indien de betrokkene van mening is dat de bepalingen van dit privacybeleid niet worden nageleefd of andere redenen heeft tot klagen met betrekking tot de verwerking van persoonsgegevens, kan de betrokkene een klacht indienen op de wijze zoals beschreven in de privacyverklaring.

De betrokkene kan ook een klacht indienen bij de Autoriteit Persoonsgegevens indien de betrokkene van mening is dat WAG gegevensverwerkingen doet in strijd met de AVG.

6.7 Dataminimalisatie en bewaartermijnen

WAG verwerkt persoonsgegevens alleen wanneer dat echt nodig is. We hanteren het principe van dataminimalisatie: niet meer gegevens verzamelen of bewaren dan strikt noodzakelijk. Dit is vastgelegd in ons **dataretentie beleid**, waarin staat hoe lang verschillende soorten gegevens bewaard mogen worden voordat ze worden verwijderd.

Het beleid geldt voor zowel digitale (gestructureerde) als minder gestructureerde data, zoals e-mails of documenten. Bij het opstellen van het **dataretentie beleid** is rekening gehouden met de wettelijke bewaartermijnen en de AVG. Dit beleid sluit nauw aan op ons privacybeleid.

6.8 Beveiligingsincidenten en datalekken

We vinden het belangrijk dat persoonsgegevens veilig worden verwerkt. Daarom maken we alle medewerkers bewust van het belang van een zorgvuldige omgang met data.

6.8.1 Melden van incidenten

Als een medewerker merkt dat persoonsgegevens per ongeluk toegankelijk zijn geworden voor onbevoegden, of als beveiligingsmaatregelen niet goed gewerkt hebben, moet dit meteen gemeld worden aan de compliance officer. Die verwerkt de melding in ons **incidentenregister datalekken**.

6.8.2 Datalekken

Wanneer bij een beveiligingsincident persoonsgegevens zijn betrokken, spreken we van een datalek. De compliance officer beoordeelt of het datalek moet worden gemeld bij de Autoriteit Persoonsgegevens (AP). Dit gebeurt alleen als het incident risico's oplevert voor de privacy van betrokkenen. Bij twijfel wordt advies gevraagd aan het bestuur en de kwaliteitsbepaler.

Als een melding nodig is, moet deze binnen **72 uur** na ontdekking worden gedaan. Ook het bestuur wordt hierover geïnformeerd. Als het risico voor de betrokken personen groot is, zijn we bovendien verplicht deze betrokkenen zelf op de hoogte te stellen.

Als wij persoonsgegevens verwerken namens een andere partij (dus als verwerker), volgen we de afspraken die daarover zijn vastgelegd in de verwerkersovereenkomst. In die gevallen melden wij incidenten aan de opdrachtgever.

We evalueren periodiek de meldingen en leren van incidenten, zodat we onze beveiliging steeds verder kunnen verbeteren.

7 bijlage I – SIRA-methodiek en risk appetite WAG

Ons kantoor maakt gebruik van de SIRA-methodiek om privacyrisico's op een gestructureerde manier in kaart te brengen en te beheersen. Hierbij bepaalt het bestuur welke risico's aanvaardbaar zijn en welke aanvullende maatregelen nodig zijn. Dit wordt aangeduid als de risk appetite: de mate van risico die wij bereid zijn te accepteren bij het nastreven van onze doelstellingen.

Binnen SIRA wordt gewerkt met vier risiconiveaus, elk gekoppeld aan een aanpak:

Bruto risico	**Aanpak (risk appetite)**
Zeer hoog	Stoppen
Hoog	Direct aanpakken
Gemiddeld	Beheersen of overdragen
Laag	Accepteren

De risk appetite kan per risico verschillen en wordt aangepast als er interne of externe ontwikkelingen zijn. Alleen het bestuur kan de risk appetite wijzigen.

De AVG biedt ruimte om een risico-afhankelijke benadering toe te passen bij privacy. Daarbij kijken we naar de **aard, omvang, context** en het **doel** van de gegevensverwerkingen binnen onze organisatie.

Aspect	**Toelichting**
Aard	Als dienstverlener is vertrouwelijkheid essentieel. We verwerken soms ook bijzondere persoonsgegevens, zoals medische gegevens, afhankelijk van de aard van de opdracht.
Omvang	Bij vrijwel al onze diensten verwerken we persoonsgegevens. Het aantal betrokkenen (zoals klanten en hun medewerkers) kan in de duizenden lopen.
Context	We verwerken uiteenlopende gegevens, van HR-informatie tot klantdata in financiële dossiers.
Doel	Gegevens worden verwerkt voor twee hoofddoelen: 1) als werkgever en 2) bij het leveren van zakelijke diensten.

Gezien deze factoren is er sprake van een **gemiddeld bruto risico** op het gebied van privacy. Dat betekent dat wij maatregelen treffen om dit risico te beheersen. Deze aanpak en de bijbehorende scenario's zijn uitgewerkt binnen onze **SIRA**.

8 Bijlage II - visuele weergave PDCA cylus