GEMEENTE WEERT

Privacy doet ertoe!

Privacybeleid gemeente Weert

2023-2026

Inhoud

Hoofdstuk 1 Inleiding

Privacy is een grondrecht, dit recht is geregeld in artikel 10 Grondwet. In dit hoofdstuk wordt uiteengezet waar we het over hebben wanneer we spreken over privacy en de Algemene Verordening Gegevensbescherming. Daarnaast wordt stil gestaan bij de relatie tussen privacy (AVG), informatiebeveiliging en andere wetgeving. Tevens wordt ingezoomd op de missie en ambitie inzake privacy van de gemeente Weert.

1.1 Wat is privacy?

Privacy in deze context gaat over de rechten en persoonlijke vrijheden van ons allemaal. De essentie van privacy is dat informatie over ons doen en laten binnen de oorspronkelijke context blijft én dat organisaties transparant zijn over hoe zij omgaan met gegevensverwerkingen.

Binnen de gemeente Weert werken ambtenaren met (bijzondere) persoonsgegevens. Privacy raakt dus de gehele gemeentelijke organisatie, ongeacht de functie. Het doel van dit privacybeleid is om te beschrijven hoe wij aantoonbaar op een juiste wijze omgaan met persoonsgegevens. Door dit privacybeleid (en aanvullende beleidsdocumenten en instructies) op te stellen én uit te dragen weet iedereen die werkzaam is bij de gemeente Weert en onze externe partners welke uitgangspunten bij de gemeente gelden. Hoe eenieder zich moet gedragen ten aanzien van privacy en in het bijzonder het verwerken van (bijzondere) persoonsgegevens.

Door dit privacybeleid uit te dragen is de gemeente Weert van betekenis voor haar inwoners en medewerkers. Privacy doet ertoe!

1.2 De Algemene Verordening Gegevensbescherming

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Dit is een Europese verordening. Het doel van de AVG is om de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie te waarborgen.

De AVG heeft rechtstreekse werking binnen de gehele Europese Unie. Daardoor harmoniseert deze verordening de regels voor de bescherming van persoonsgegevens. Op specifieke punten biedt de AVG de lidstaten de ruimte om nadere invulling te geven aan bepalingen uit de AVG. Deze invulling geschiedt via zogenaamde uitvoeringswetten. In Nederland is dit de Uitvoeringswet AVG.

De Autoriteit Persoonsgegevens (AP) is de Nederlandse onafhankelijke toezichthouder op het gebied van privacywetgeving en heeft bevoegdheden om te acteren.

Dit privacybeleid gaat in op de verplichtingen die de AVG stelt aan de gemeente Weert.

1.3 Privacy en informatiebeveiliging

Privacy gaat hand in hand met informatiebeveiliging. Het zijn twee verschillende begrippen, maar wel met een gemeenschappelijk raakvlak. Waar informatiebeveiliging gaat over het beveiligen van bedrijfsinformatie in de breedste zin van het woord, gaat privacy specifiek over het beschermen van persoonsgegevens. Zowel informatiebeveiliging als privacy vragen om een risico-gedreven aanpak.
Wel gelden er verschillende normenkaders voor beide vakgebieden. Waar de Baseline

Informatiebeveiliging Overheid (BIO) van belang is voor informatiebeveiliging, is de AVG van groot belang in het domein van privacy.

1.4 De AVG versus andere wetgeving

De AVG en de uitvoeringswet AVG beschrijven wat wel en niet mag in het kader van privacy, onder welke voorwaarden, welke plichten organisaties hebben en welke rechten burgers hebben. Dit is de basis, wat gezien kan worden als kapstok.

De gemeente Weert voert publiekrechtelijke taken uit. Deze taken vloeien voort uit vele sectorwetten, denk aan de wet Maatschappelijke Ondersteuning 2015 (WMO 2015), de Jeugdwet en de wet Basisregistratie Personen (wet BRP). In de sectorale wetten kan beschreven staan hoe met persoonsgegevens moet worden omgegaan. Dit is een invulling/aanvulling van de (open) normen die staan in de AVG, het zijn de jassen aan de kapstok.

De gemeente Weert heeft daarnaast privaatrechtelijke taken en voert hiervoor bedrijfsvoeringstaken uit. Hiervoor geldt naast de AVG ook de algemene wet- en regelgeving.

1.4.1 Wet politiegegevens

Voor de boa's gelden er twee verschillende privacy regimes: de AVG en de Wet politiegegevens (Wpg). Boa's hebben vaak meerdere taken en verwerken verschillende soorten persoonsgegevens. De persoonsgegevens die de boa verwerkt in zijn rol als toezichthouder vallen onder de AVG. Sinds 2019 vallen de persoonsgegevens die de boa verwerkt als opsporingsambtenaar onder de Wpg.

Voor persoonsgegevens die onder de Wpg worden verwerkt (opsporing) gelden o.a. andere verwerkingstermijnen en andere regels voor het delen van gegevens, dan onder de AVG. De gegevenshuishouding, systemen en werkprocessen moeten dus anders worden ingericht dan bij de verwerkingen die in het kader van toezicht (AVG) worden gedaan. Tevens kent de Wpg een auditplicht. Eén keer per jaar dient er een interne audit plaats te vinden en één keer in de vier jaar een externe audit. Het externe auditrapport dient gedeeld te worden met de Autoriteit Persoonsgegevens.

De gemeente Weert heeft boa's in dienst die verwerkingen uitvoeren die onder het regime van de Wpg vallen. Daarom dient de gemeente Weert er zorg voor te dragen dat de gegevenshuishouding, systemen en werkprocessen die van toepassing zijn op de werkzaamheden van boa's Wpg-proof zijn ingericht/opgesteld.

1.5 Privacy missie en privacy ambitie

Zorgvuldig omgaan met persoonsgegevens hoort bij de werkzaamheden van alle medewerkers van de gemeente Weert. Hieronder wordt de missie en ambitie inzake privacy genoemd:

Missie op privacy: Gemeente Weert werkt op een evenwichtige manier met persoonsgegevens. Naar de intentie van de AVG, met doelbinding en transparantie.

Ambitie op privacy: De gemeente Weert voldoet in 2026 op alle privacy-thema's genoemd in het borgingsproduct van het IBD op privacyvolwassenheidsniveau 3.[1]

1.6 Begrippenlijst

Een aantal begrippen komen meerdere keren voor in het privacybeleid. Daarom worden deze begrippen hieronder toegelicht.

Autoriteit Persoonsgegevens: De Nederlandse toezichthouder met betrekking tot de naleving van de AVG.

AVG: Algemene Verordening Gegevensbescherming

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

Datalek: Wanneer persoonsgegevens in handen vallen van derden die geen toegang tot de persoonsgegevens mogen hebben, of als er een vermoeden is dat dit gaat gebeuren.

Een datalek is niet enkel een inbreuk op de beveiliging. Een datalek kan ook het verlies van persoonsgegevens zijn zonder back-up, het wijzigen van persoonsgegevens, het open en bloot 'laten rondslingeren' van documenten met persoonsgegevens erin op bureau of beeldscherm, of het versturen van een e-mail naar een verkeerd emailadres.

Data Protection Impact Assessment (DPIA): Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Tevens wordt beschreven welke maatregelen genomen dienen te worden om de geconstateerde risico's te mitigeren.

Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Het begrip persoonsgegevens moeten we dus ruim opvatten. Niet alleen NAW-gegevens, e-mail adres, BSN, postcode en huisnummer, IP-adres zijn persoonsgegevens. Maar ook combinaties van gegevens: bijvoorbeeld leeftijd, geslacht, postcode, (huur)huis, gezinssamenstelling.

RASCI-rollen:
R = Responsible/Verantwoordelijk: Degene die verantwoordelijk is voor de uitvoering en die verantwoording afgelegd aan de accountable persoon.
A = Accountable/Eindverantwoordelijk: Er is slechts één persoon Accountable / (eind)verantwoordelijk, degene die bevoegd is. Deze bepaalt de taak, het doel en middelen (en of preventieve maatregelen getroffen worden). Geeft goedkeuring aan het resultaat (eindoordeel vellen, vetorecht). Deze wordt aangesproken als het risico zich voordoet.
S= Support/Ondersteunend: Deze partij geeft ondersteuning aan het proces of project (ontwerp) en voert lijnwerkzaamheden uit (implementatie of regelen van activiteiten).
C = Consulted/Geraadpleegd: Deze partij geeft (mede) richting aan het resultaat, hij/zij wordt voorafgaand aan beslissingen of acties (verplicht) geraadpleegd. Dit is

[1] Handreiking AVG borgingsproduct 2.0, p. 9.

tweerichtingscommunicatie.
I = Informed/Geïnformeerd: De partij die geïnformeerd wordt over de beslissingen, over de voortgang, bereikte resultaten etc. Dit is eenrichtingscommunicatie.

Register van verwerkingsactiviteiten: Het register dat wordt bijgehouden door een verwerkingsverantwoordelijke waarin de verwerkingsactiviteiten worden bijgehouden die onder hun verantwoordelijkheid plaatsvinden.

UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming

*Verwerker***:** De persoon of organisatie die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerkingsverantwoordelijke: Een persoon of organisatie die, alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking: Het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, inzien (raadplegen), gebruiken, verstrekken (doorsturen, verspreiden), combineren, afschermen, wissen of vernietigen van persoonsgegevens. Al dan niet geautomatiseerd. Zowel op papier, digitaal als mondeling.

Hoofdstuk 2 Beginselen AVG

Op grond van artikel 5 AVG is de gemeente Weert verplicht de AVG-beginselen in acht te nemen bij het verwerken van persoonsgegevens. Hieronder worden puntsgewijs deze beginselen uiteengezet:

2.1. Rechtmatig, behoorlijk en transparant (sub a):

Rechtmatigheid
Een verwerking is alleen rechtmatig indien en voor zover aan de voorwaarden is voldaan zoals opgenomen in artikel 6 AVG, te weten:

- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking (sub a);
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was (sub b);
- Om een verplichting na te komen die in de wet staat (sub c);
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden (sub d);
- Voor de goede invulling van de gemeentelijke taak (sub e);
- Indien een zorgvuldige belangenafweging dit uitwijst (sub f).

De gemeente Weert verwerkt persoonsgegevens zoveel als mogelijk vanuit de publieke taak welke zij heeft op grond van aan haar opgelegde taken (sub e). De gemeente Weert verwerkt ook persoonsgegevens wanneer de wet haar daartoe verplicht (sub c).

Behoorlijk en transparantie
De gemeente Weert wil het belang van privacy uitdragen en een betrouwbare gemeente zijn door in ons handelen de privacy van betrokkenen te eerbiedigen en transparant te zijn over de manier waarop wij dit doen.
Op grond van het transparantiebeginsel moeten informatie en communicatie in verband met de verwerking van die persoonsgegevens eenvoudig toegankelijk en begrijpelijk zijn voor betrokkenen. Er moet hierbij heldere en eenvoudige taal worden gebruikt.
De gemeente Weert zorgt er zoveel mogelijk voor dat betrokkenen worden geïnformeerd over de doeleinden van de verwerkingen. Vaak gebeurt dit al doordat de betrokkene zijn/haar gegevens zelf doorgeeft op een aanvraagformulier. Hierop staat vaak al vermeld welke persoonsgegevens nodig zijn en voor welk doel. Als de gemeente persoonsgegevens verwerkt die ze niet van de betrokkene heeft verkregen, stelt de gemeente de betrokkene zo veel mogelijk op de hoogte.

In het kader van transparantie is er op de website van de gemeente Weert een privacyverklaring geplaatst, waarin uitleg wordt gegeven waarom en hoe de gemeente persoonsgegevens verwerkt. Tevens is op de website van de gemeente het register van verwerkingsactiviteiten te vinden.

2.2 Doelbinding en verenigbaarheid (sub b)

Persoonsgegevens mogen enkel worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. De verwerkingsdoeleinden staan vermeld in het register van verwerkingsactiviteiten. Wanneer gegevens later voor een ander doel worden gebruikt, dan moet dit nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel.

2.3 Gegevensminimalisatie (sub c)

Gegevensminimalisatie wordt ook wel dataminimalisatie genoemd. Het betekent dat de gemeente niet meer persoonsgegevens mag verzamelen dan strikt noodzakelijk is voor het beoogde doel. Dit sluit aan bij de begrippen proportionaliteit en subsidiariteit. Deze begrippen betekenen dat we het verwerken van persoonsgegevens zo klein mogelijk houden en dat het verwerken van gegevens in verhouding staat tot het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt.

In bepaalde wet- en regelgeving is soms bepaald welke persoonsgegevens noodzakelijk zijn om het doel te bereiken. Wanneer dit niet het geval is maakt gemeente Weert zelf deze afweging. Hierbij worden enkel de gegevens verwerkt die noodzakelijk zijn om het doel te bereiken.

2.4 Juistheid (sub d)

Gemeente Weert dient alle redelijke maatregelen te nemen om ervoor te zorgen dat onjuiste persoonsgegevens worden gecorrigeerd of vernietigd.

2.5 Opslagbeperking (sub e)

Er dient te worden gezorgd dat de opslagperiode (ook wel de bewaartermijn genoemd) van persoonsgegevens tot een strikt minimum worden beperkt. Wanneer er persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel moeten deze zo snel mogelijk worden vernietigd. Dit houdt in dat deze gegevens verwijderd worden of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren (anonimiseren).

Het loopt uiteen hoelang gemeente Weert persoonsgegevens bewaart. De Archiefwet, de Selectielijst van de VNG en diverse andere wetten verplichten de gemeente om persoonsgegevens voor een minimale of maximale termijn te bewaren. In het register van verwerkingsactiviteiten staat de bewaartermijn genoemd. Tijdens deze bewaartermijn zorgt de gemeente voor een zorgvuldige en beveiligde opslag. Na verloop van de verplichte bewaartermijn worden de gegevens vernietigd**.**

2.6 Integriteit en vertrouwelijkheid (sub f)

De gemeente Weert gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Conform artikel 32 AVG zorgt de gemeente daarbij voor passende beveiliging van persoonsgegevens. In de Baseline Informatiebeveiliging Overheid (BIO) staan de verplichtende voorwaarden voor gemeenten om te voldoen aan het begrip passende beveiliging. In het Informatiebeveiligingsbeleid van de gemeente Weert wordt hier verder invulling aangegeven.

2.7 Privacy by design en privacy by default

De gemeente Weert hanteert de principes ‘privacy by design’ en ‘privacy by default’ bij haar verwerkingen. Door vanaf het begin na te denken over de mogelijke privacyvraagstukken en dit mee te nemen in de inrichting verkleinen we de eventuele privacyrisico’s.

Het beginsel ‘privacy by design’ houdt in dat de bescherming van persoonsgegevens bij de ontwikkeling van producten, procedures en diensten die gepaard gaan met de verwerking van persoonsgegevens, wordt meegenomen en ingebouwd. Borging hiervan

gebeurt in het inkoopproces, het wijzigingsbeheer van systemen en het melden van aanzienlijke risico's in het Weerter stuurmodel.

Het beginsel 'privacy by default' houdt in dat de standaardinstellingen bij de inrichting van (nieuwe) systemen zodanig zijn gekozen dat de bescherming van persoonsgegevens wordt gewaarborgd. Dit houdt in dat waar dit mogelijk is niet meer persoonsgegevens worden gedeeld/getoond dan noodzakelijk is voor het uitoefenen van de taak/doel. Borging hiervan gebeurt in het inkoopproces, het wijzigingsbeheer van systemen en het melden van aanzienlijke risico's in het Weerter stuurmodel.

Hoofdstuk 3 Verantwoordelijkheden, taken en bevoegdheden

Op grond van artikel 5 lid 2 AVG is de verwerkingsverantwoordelijke eindverantwoordelijk voor de naleving van de AVG. In dit hoofdstuk wordt uiteengezet wie in de organisatie welke verantwoordelijkheden en taken hebben ten aanzien van de naleving van de AVG.

3.1 Verantwoordingsplicht

Alle bestuursorganen van de gemeente zijn verantwoordelijk voor de naleving van de privacywet- en regelgeving, zoals de AVG en het privacybeleid, ieder voor zover het haar bestuurlijke taken betreft. De bestuursorganen van de gemeente zijn de gemeenteraad, het college van burgemeester en wethouders (het college van B&W) en de burgemeester.

3.2 Rollen

Om daadwerkelijk te kunnen waarborgen dat privacybescherming ingebed wordt in de organisatie is het noodzakelijk dat alle in de organisatie werkzame personen (inclusief externen en inhuur), ieder vanuit hun eigen rol worden bezien. Hieronder worden deze verschillende rollen (met hun verantwoordelijkheden) om uitvoering te geven aan dit privacybeleid kort uiteengezet.[2]

Om de rollen en verantwoordelijkheden van de personen bij lijnwerkzaamheden inzichtelijk te maken, hanteert de gemeente Weert de RASCI-methode. In bijlage 1 is daarom het RASCI-model privacyrollen toegevoegd.

3.2.1. Gemeenteraad

De gemeenteraad heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan hen toekent.

3.2.2. College van B&W en de burgemeester

Voor de publiekrechtelijke taken is het college van burgemeester & wethouders (bestuurlijk) eindverantwoordelijk. De burgemeester is de portefeuillehouder voor de uitvoering van de AVG binnen de gemeente.

3.2.3 Gemeentesecretaris

De gemeentesecretaris/algemeen directeur heeft een belangrijke rol in het borgen van privacy. Hij/zij heeft de gemandateerde ambtelijke verantwoordelijkheid voor privacy en is verantwoordelijk voor de juiste implementatie van privacy in de bedrijfsprocessen en (informatie)systemen.

[2] De verantwoordelijkheden, taken en bevoegdheden vloeien voort uit het beleidsdocument GBD-301 privacy rollen.

De gemeentesecretaris/algemeen directeur zorgt ervoor (dat):

- Dat hij/zij de rol kan nemen als verantwoordelijke;
- De controle op de privacy binnen de organisatie is gewaarborgd;
- Is het eerste aanspreekpunt voor de functionaris gegevensbescherming (FG);
- De organisatie in staat is om de verschillende verantwoordelijkheden inzake; privacy te dragen
- Er een duidelijke functiescheiding is tussen uitvoerende, controlerende en beleidsbepalende taken;
- Het privacy bewustzijn binnen de organisatie bevorderd wordt;
- Er een (actueel) privacybeleid is;
- Er gestuurd wordt op privacyrisico's;
- De nodige middelen ter beschikking worden gesteld voor het vervullen van de taken en het in stand houden van de deskundigheid;
- Er (wordt geïnformeerd en) wordt gerapporteerd over de betrouwbaarheid van privacy aan de portefeuillehouder en het college (via de ENSIA);
- Er in overleg met de FG bepaald wordt welke rol de FG ten opzichte van de rekenkamer en de raad heeft.

3.2.4 DT/CMT

De operationele verantwoordelijkheid voor privacy is gemandateerd aan het DT/CMT. De managers zijn verantwoordelijk voor een juiste implementatie en naleving van privacy in bedrijfsprocessen, (informatie)systemen en projecten. Zij wijzen voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan.

Het DT/CMT zorgt ervoor dat:

- Het privacy bewustzijn binnen de organisatie wordt bevorderd;
- De medewerkers ondersteund worden met kennis over privacy bij het uitvoeren van hun taken door de nodige middelen beschikbaar te stellen;
- Het privacybeleid wordt opgesteld, uitgedragen en uitgevoerd;
- Het privacybeleid periodiek wordt geëvalueerd en bijgesteld;
- Er gestuurd wordt op de privacyrisico's;
- Er een melding wordt gemaakt bij het datalekteam wanneer er sprake is van een (mogelijk) datalek. De melding dient afgehandeld te worden conform de procedure melden datalekken van de gemeente Weert;
- Zorgt voor het vrijmaken van privacy budget en resources voor de afdeling.

3.2.5 Functionaris gegevensbescherming

De functionaris gegevensbescherming (FG) heeft een onafhankelijke positie binnen de organisatie. De FG is in ieder geval verantwoordelijk voor het houden van toezicht op en adviseren van de organisatie over de juiste en zorgvuldige omgang met persoonsgegevens. Dit betekent dat de FG bij alle processen waar persoonsgegevens worden verwerkt betrokken moet worden door de organisatie.

De FG zorgt ervoor dat (artikel 39 AVG):

- Rapporteert rechtstreeks aan de directeur bedrijfsvoering/gemeentesecretaris;
- Hij/zij voor afdelingsspecifieke zaken de betreffende DT/CMT-er direct kan benaderen;
- In geval van crisis of ernstige gebreken mag de FG direct aan de portefeuillehouder privacy en het college rapporteren;

- Zorgt voor samenwerking met Autoriteit Persoonsgegevens en is het contactpunt voor de Autoriteit Persoonsgegevens;
- Zorgt voor waarborging van privacy van de medewerker;
- Zorgt voor bewustwording, het informeren van en het adviseren over privacywetgeving aan de organisatie;
- Maakt een jaarverslag voor de gemeentesecretaris;
- Ziet toe op de (adequate informatiebeveiliging en) gegevensverwerkingen en geeft hierover advies aan de organisatie en het college;
- De FG werkt nauw samen met de PO en de CISO.

3.2.6 Privacy officer

De privacy officer (PO) heeft gemeentebreed uitvoerende taken op gebied van privacy. Door het aanstellen van de PO wordt in de organisatie gewaarborgd dat de wettelijke privacy taken worden uitgevoerd. De PO is het aanspreekpunt voor alle collega's ten aanzien van privacy. De PO dient bij alle processen waar persoonsgegevens worden verwerkt betrokken te worden door de organisatie.

De PO zorgt ervoor dat:

- Hij/zij ondersteunt bij de uitvoering van acties die bijdragen aan de bewustwording binnen de organisatie op het gebied van privacy;
- De procedure melden datalekken actueel blijft. De PO is voorzitter van het datalekteam;
- Een procedure voor rechten van betrokkenen wordt opgesteld en actueel blijft;
- Er een register van verwerkingsactiviteiten is opgesteld en wordt bijgehouden;
- De standaard verwerkingsovereenkomst beschikbaar is voor de organisatie en dat deze overeenkomst actueel blijft. Daarnaast biedt de PO ondersteuning bij vragen over de verwerkersovereenkomst;
- Het privacybeleid actueel blijft;
- Zorgt voor het opstellen van een organisatieplan privacy (privacy plan) en een jaarplanning;
- De uitvoering van privacy taken wordt gecoördineerd;
- Er een checklist DPIA is opgesteld en actueel blijft. Daarnaast biedt de PO ondersteuning bij de uitvoering van de (checklist) DPIA's;
- Hij/zij is het aanspreekpunt voor medewerkers over het onderwerp privacy, samen met de FG;
- Werkt nauw samen met de FG en met de CISO;
- Stemt af met de informatiemanagers t.a.v. het benodigde organisatiebrede informatiebeveiliging- en privacy budget (bijv. voor een privacy beheersysteem, privacy bewustwording/training budget, externe kennis of ondersteuning van/bij bijv. DPIA's).

3.2.7 Privacy contactpersonen

De privacy contactpersoon (PC) ondersteunt het afdelingshoofd/organisatieonderdeel met het zorgvuldig omgaan met de privacy van betrokkenen en eventuele privacy vragen die er spelen binnen de afdeling. Voor beantwoording van de vragen kunnen PO en/of FG om advies gevraagd worden. Voor de PO en/of de FG is de PC de ingang voor vragen binnen de afdeling. De PC heeft inzicht in specifieke wet- en regelgeving in relatie tot de AVG en ondersteunt in de naleving ervan.

De privacy contactpersoon is voor zijn/haar afdeling/team:

- De vraagbaak voor collega's m.b.t. privacy vragen en bevordert de privacy bewustwording;
- De PC is voor de PO en de FG m.b.t. vragen de contactpersoon;
- De contactpersoon m.b.t. datalekken (de persoon die ondersteunt bij het melden en afhandelen van datalekken);
- De persoon die ondersteunt dat maatregelen uit het privacybeleid voor de betreffende afdeling/team processen worden uitgevoerd.

Eén keer per kwartaal vindt er een overleg plaats tussen de PO, FG en alle privacy contactpersonen. Doel van het overleg is: kennisdeling én bewustwording, generieke privacy- en informatiebeveiligingszaken, proceswijzigingen en systeemkoppelingen bespreken.

3.2.8 Medewerkers

Elke medewerker draagt zorg voor privacy binnen zijn/haar functie en dagelijks werk. Medewerkers zijn operationeel verantwoordelijk voor privacy.

Medewerkers zorgen ervoor dat:

- Ze bewust bezig zijn met het onderwerp privacy binnen het dagelijks werk;
- Zij op de hoogte zijn waar men terecht kan met vragen omtrent privacy;
- Ze datalekken melden bij het datalekteam;
- Ze bij een datalek alle support leveren (melding maken, gegevens aanleveren, onderzoek doen);
- Ze de communicatiekanalen en –middelen gebruiken zoals de gemeente Weert voorschrijft;
- Ze werken vanuit het zaaksysteem en andere (back end) systemen. Opslag van (in concept versies van) officiële documenten op andere plaatsen is niet toegestaan, zoals bijvoorbeeld op afdelingsschijven, persoonlijke folders, in e-mails.

3.2.9 Datalekteam

Het datalekteam is geformeerd om de organisatie te ondersteunen bij de tijdige en juiste afhandeling van datalekken binnen de wettelijke verplichtingen van de AVG, oftewel het binnen 72 uur melden van het incident aan de Autoriteit Persoonsgegevens indien het een meldingsplichtig datalek betreft en/of het informeren van de betrokkenen. De vaste kern van het datalekteam bestaat uit een eerste en tweede lijn. Het datalekteam volgt de vastgestelde procedure melden datalekken.

De vaste kern van het datalekteam bestaat uit:

1. Eerste lijn: PO, CISO en FG. Deze rollen zijn echter parttimefuncties. Hiermee kan niet worden voldaan aan de beschikbaarheidseis. Vandaar dat bij afwezigheid en/of andere prioriteiten van de eerste lijn, de tweede lijn de datalekmeldingen oppakken en ondersteunen bij de afhandeling.
2. Tweede lijn: de gegevensbeheerder en de senior applicatiebeheerders (o.a. van Djuma en Motion) van afdeling Informatie.

3.2.10 AVG-team

Het AVG-team bestaat uit: PO, CISO, FG, afdelingshoofd Informatie, procesmanager en gegevensbeheerder. Eén keer per week komt het AVG-team bij elkaar om knelpunten rondom privacy (en informatiebeveiliging) met elkaar te bespreken. Daarnaast wordt de voortgang van privacy/informatiebeveiligingsacties besproken.

Het AVG-team heeft een privacy plan opgesteld. In het privacy plan staan de privacy acties beschreven die uitgevoerd dienen te worden zodat de gemeente aan het privacybeleid voldoet. Elk jaar wordt het privacy plan geactualiseerd door het AVG-team.

Hoofdstuk 4 Inbedding van privacy in de organisatie

Op grond van artikel 5 lid 2 AVG dient de gemeente Weert aan te tonen dat een verwerking aan de AVG voldoet. De gemeente dient rekenschap af te (kunnen) leggen. In dit hoofdstuk worden de punten uiteengezet die de gemeente genomen heeft.

4.1 Register van verwerkingsactiviteiten

Op grond van artikel 30 AVG is de gemeente Weert verplicht een register van verwerkingsactiviteiten met alle verwerkingen die plaatsvinden onder onze verantwoordelijkheid op te stellen en bij te houden. In artikel 30 lid 1 AVG is uiteengezet welke gegevens het register bevat. Een structurele verwerking van persoonsgegevens dient altijd eerst aan de privacy officer gemeld te worden voordat de verwerking begint.

Het register van verwerkingsactiviteiten is een levend document. Het register wordt o.a. ingezet voor een efficiënte behandeling van een verzoek van een betrokkene (inzagerecht, correctierecht, recht om vergeten te worden).

4.2 Persoonsgegevens delen met derden

De gemeente werkt veel samen met externe partijen. Hiervoor kan het nodig zijn om persoonsgegevens met elkaar te delen. Wanneer persoonsgegevens met andere partijen worden gedeeld gebeurt dit altijd binnen de kaders en uitgangspunten zoals gesteld in dit beleid.

Conform de AVG bepaalt de eindverantwoordelijke welke persoonsgegevens verwerkt worden, voor welk doel en welke middelen daarvoor worden ingezet. Wanneer de gemeente voor een verwerking met persoonsgegevens samenwerkt met derden, bekijkt de gemeente Weert of deze partner een verwerker is of een (gezamenlijke) verwerkingsverantwoordelijke is. De (eind)verantwoordelijke medewerker doorloopt de beslisboom ‘Verwerkersovereenkomst nodig?’ Deze beslisboom is te vinden via het intranet van de gemeente. Gemeente Weert sluit met haar verwerkers een verwerkersovereenkomst. Wij hanteren de laatste versie van de standaard verwerkersovereenkomst vastgesteld door de VNG.

Indien sprake is van gezamenlijke verwerkingsverantwoordelijkheid is de gemeente verplicht op grond van de AVG om een onderlinge regeling op te stellen waarin de respectievelijke verplichtingen zijn vastgelegd. Hiervoor wordt de modelovereenkomst gezamenlijke verwerkingsverantwoordelijken van de VNG gebruikt.

Het sluiten van een verwerkersovereenkomst of overeenkomst gezamenlijke verwerkingsverantwoordelijken wordt geborgd vanuit het inkooptraject voor systemen.

Wanneer een externe/inhuur uit hoofde van zijn functie geacht wordt namens de gemeente persoonsgegevens te verwerken, dient hij daarvoor vóóraf een geheimhoudingsverklaring te ondertekenen.

4.3 Datalekregistratie en datalekmelding

Wanneer een (vermoeden van een) datalek zich voordoet dient de gemeente snel en efficiënt in actie te komen. Er moet nagegaan worden of er daadwerkelijk een datalek heeft plaatsgevonden. Bij het vaststellen van een datalek wordt o.a. de vraag gesteld of de persoonsgegevens waren beschermd door adequate technische maatregelen die de kans op identiteitsfraude, discriminatie of andere vormen van misbruik beperkten.

Indien een datalek heeft plaatsgevonden is de gemeente Weert ingevolge artikel 33 AVG wettelijk verplicht om een datalek te melden aan de Autoriteit Persoonsgegevens (AP)

wanneer het incident waarschijnlijk een risico vormt voor de rechten en vrijheden van de betrokkene(n). Deze melding moet gebeuren binnen 72 uur nadat kennis van het datalek is genomen. Indien de melding later dan 72 uur plaatsvindt zal er een motivering voor de vertraging bij de melding worden gevoegd. Wanneer een datalek een groot risico vormt voor de rechten en vrijheden van de betrokkenen zullen wij deze betrokkenen informeren over het incident, tenzij een mededeling op grond van artikel 34 lid 2 AVG niet van de gemeente kan worden gevergd. Gemeente Weert communiceert altijd aan de betrokkenen in eenvoudige en duidelijke taal.

De gemeente Weert heeft een procedure melden datalekken opgesteld. De gemeentesecretaris, of diens vervanger, beslist of het datalek gemeld moet worden bij de Autoriteit Persoonsgegevens en/of bij de betrokkene(n).

Gemeente Weert registreert alle datalekken in een datalekkenregister, documenteert de gehele afhandeling in het zaaksysteem en evalueert bestaande datalekken. Zo leren we van datalekken en proberen we (identieke) datalekken te voorkomen.
Daarnaast sluiten wij (indien nodig) verwerkersovereenkomsten met opdrachtnemers en andere externe partijen die persoonsgegevens verwerken. In deze verwerkersovereenkomsten staan afspraken over hoe de privacy van de betrokkenen moeten worden beschermd en hoe moet worden gehandeld bij het constateren van een (vermoedelijke) datalek.

4.4 Data protection impact assessment (DPIA)

Ingevolge artikel 35 AVG is de verwerkingsverantwoordelijke verplicht een DPIA uit te (laten) voeren wanneer een verwerking een hoog privacyrisico vormt voor betrokkenen. Met een Data Protection Impact Assessment (DPIA), ook wel gegevensbeschermingseffectbeoordeling genoemd, worden de effecten en risico’s van nieuwe of bestaande hoog privacyrisico verwerkingen beoordeeld op de bescherming van de privacy. Tevens wordt beschreven welke maatregelen genomen dienen te worden om de geconstateerde risico's te mitigeren. Bij de DPIA wordt met name de oorsprong, de aard, het specifieke karakter en de ernst van dat risico van het verwerken van persoonsgegevens vooraf geëvalueerd door de verwerkersverantwoordelijke.

In de procedure DPIA wordt beschreven op welke wijze de gemeente Weert een DPIA oppakt en uitvoert. Verantwoordelijk en trekker van de uitvoering van een (checklist) DPIA is het CMT, en dit kan worden belegd bij een procesverantwoordelijke of projectleider.

4.5. Communicatie en bewustwording

<u>Communicatie- en bewustwordingsplan privacy en informatiebeveiliging</u>
De gemeente Weert heeft een communicatie- en bewustwordingsplan inzake privacy en informatiebeveiliging opgesteld. Het doel van dit plan is om collega’s te informeren/instrueren en hun kennis over de thema’s privacy en informatiebeveiliging te vergroten. Daarmee willen we ervoor zorgen dat de collega’s zich bewust zijn van de risico’s en hoe ze veilig en verantwoord met informatie kunnen omgaan. De thema’s privacy en informatiebeveiliging vullen elkaar op verschillende manieren aan en/of liggen in elkaars verlengde. Op de punten waar de thema’s elkaar raken, wordt samengewerkt in de communicatie.

De bewustwordingsactiviteiten worden voor één jaar gepland. Het plan wordt jaarlijks geactualiseerd door het AVG-team.

Bewustwordingscampagne privacy en informatiebeveiliging

In 2022 is de gemeente Weert gestart met een e-learning omtrent privacy en informatiebeveiliging. Tijdens deze bewustwordingscampagne krijgen alle medewerkers van de gemeente wekelijks een e-mail met daarin een vraag omtrent privacy of informatiebeveiliging. Elk kwartaal ontvangen alle medewerker een e-mail met hierin een korte training omtrent een specifiek onderwerp inzake privacy of informatiebeveiliging.

Hoofdstuk 5 Rechten van betrokkenen

De AVG kent betrokkenen verschillende privacyrechten toe zodat de betrokkenen controle kunnen houden over hun eigen persoonsgegevens. Deze rechten worden rechten van betrokkenen genoemd en zijn terug te vinden in artikel 13 t/m 22 AVG. Het gaat om de volgende rechten:

- **Recht op informatie (artikel 13 en 14 AVG):** Persoonsgegevens kunnen direct (dus van de betrokkene zelf) of indirect (niet van de betrokkene zelf) zijn verkregen. De gemeente stelt zo veel mogelijk de betrokkene op de hoogte van het feit dat verwerking van zijn persoonsgegevens plaatsvindt of zal plaatsvinden en wat de doeleinden daarvan zijn. In artikel 13 en 14 AVG is beschreven welke informatie in elk geval verstrekt moet worden.

- **Recht op inzage (artikel 15 AVG):** Betrokkenen hebben de mogelijkheid om te informeren of hun persoonsgegevens worden verwerkt. In artikel 15 AVG wordt aangegeven welke informatie op grond van dat artikel inzage gegeven kan worden.

- **Recht op rectificatie (artikel 16 AVG):** Wanneer verwerkte persoonsgegevens onjuist of onvolledig zijn heeft de betrokkene het recht om deze te laten corrigeren of aan te vullen. Het verzoek wordt in behandeling genomen met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

  Wanneer daadwerkelijk rectificatie plaatsvindt, zal de gemeente iedere ontvanger aan wie deze persoonsgegevens zijn verstrekt in kennis stellen van deze rectificatie, tenzij dit onmogelijk is of onevenredig veel inspanning vraagt (zie artikel 19 AVG).

- **Recht op gegevenswissing/ "recht op vergetelheid" (artikel 17 AVG):** Betrokkenen hebben het recht om te verzoeken om (bovenmatige) persoonsgegevens te verwijderen. Het wissen van persoonsgegevens is niet altijd verplicht, bijvoorbeeld wanneer een verwerking een wettelijk plicht betreft. De uitzonderingen zijn uiteengezet in artikel 17 AVG.

- **Recht op beperking van de verwerking (artikel 18 AVG):** Het recht op beperking van de verwerking houdt in dat de gemeente (tijdelijk en onder voorwaarden) niet mag verwijderen of verwerken. De gemeente Weert informeert de betrokkene voordat de blokkade wordt opgeheven.

- **Recht op overdraagbaarheid van gegevens (artikel 20 AVG):** Het recht van overdraagbaarheid van gegevens houdt in dat betrokkene in voorkomende gevallen de mogelijkheid heeft om bij een verwerkingsverantwoordelijke een kopie van zijn persoonsgegevens dat bruikbaar is bij een andere dienstverlener op te vragen. Het recht op dataportabiliteit bestaat alleen wanneer de verwerking berust op toestemming of op een overeenkomst én de verwerking geautomatiseerd is. Gezien de (gemeentelijke) taken die gemeenten hebben zal een betrokkene slechts in zeer beperkte gevallen een geslaagd beroep kunnen doen op dit recht bij gemeenten.

- **Recht op bezwaar (artikel 21 AVG):** Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens (dit recht is niet vergelijkbaar met bezwaar op grond van de Algemene wet

bestuursrecht). De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

- **Geautomatiseerde individuele besluitvorming, waaronder profilering (artikel 22 AVG):** Uitgangspunt van artikel 22 AVG is dat er geen geautomatiseerde besluitvorming op basis van profilering mag plaatsvinden als daaraan rechtsgevolgen voor de betrokkenen (degene wiens persoonsgegevens het betreft) zijn verbonden of het besluit hem/haar in aanmerkelijke mate treft. Daarbij kan gedacht worden aan bijvoorbeeld de kredietwaardigheid van een persoon.

5.1 Indienen van een verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. De betrokkene kan een verzoek indienen via kanalen die de gemeente daarvoor heeft aangewezen. Deze kanalen staan in de privacyverklaring op de algemene website van de gemeente Weert beschreven. De indiener van het verzoek dient zich altijd te identificeren om zo aan te tonen dat de gegevens die de indiener wil inzien, corrigeren of verwijderen daadwerkelijk van hem/haar zijn.
In de procedure rechten van betrokkenen wordt beschreven hoe de gemeente Weert een AVG-verzoek oppakt en afhandelt.

Conform de AVG heeft de gemeente vier weken de tijd, vanaf het ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. In complexe situaties kan deze termijn worden verlengd met twee extra maanden. In geval van overschrijding gelden de regels van de Algemene wet bestuursrecht.

5.2 Vragen en klachten over de verwerking van persoonsgegevens

Indien er vragen zijn kan er contact opgenomen worden met de gemeente via privacy@weert.nl.

Als er klachten zijn over de verwerking van persoonsgegevens kan dit gemeld worden aan de functionaris gegevensbescherming via:

- E-mail: FG@weert.nl of;
- Schriftelijk: Gemeente Weert, t.a.v. de functionaris gegevensbescherming
  Postbus 950, 6000 AZ Weert

Bijlage 1 RASCI-model privacyrollen

RASCI-rol	**Organisatieonderdeel**	
R (Verantwoordelijkheid)	DT/CMT	
A (Eindverantwoordelijk)	College van B&W/ burgemeester--> Bestuurlijk eindverantwoordelijk	Gemeentesecretaris--> Ambtelijk eindverantwoordelijk
S (Ondersteunend)	Privacy officer, datalekteam, privacy contactpersonen, AVG-team	
C (Raadpleger)	Functionaris gegevensbescherming (onafhankelijk), privacy officer	
I (Geïnformeerd)	College van B&W, gemeenteraad, Ondernemersraad, burgers.	