gemeente kerkrade

GEMEENTEBLAD

Officiële uitgave van de gemeente Kerkrade

Nr. 63933

12 februari

2026

Privacybeleid Gemeente Kerkrade 2026 – 2029

Inleiding

De Gemeente Kerkrade werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke taken, voortvloeiende uit wet- en regelgeving, uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, Omgevingswet, openbare orde en veiligheid, burgerzaken en welzijn. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen en een steeds meer digitaliserende overheid maken het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale- en Europese wet- en regelgeving op het gebied van privacy en gegevensbescherming, waaronder de Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene Verordening Gegevensbescherming (hierna te noemen: AVG en UAVG)
De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in uitvoerende documenten zoals handreikingen, protocollen en regelingen. Dit geldt voor gemeente brede privacy-processen zoals datalekken, rechtenverzoeken maar ook voor domein-specifieke onderwerpen zoals gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning. Privacy is een vast aspect binnen procesmanagement. In alle relevante werkinstructies wordt privacy standaard en aantoonbaar verwerkt.
Naast dit door het college vastgestelde privacybeleid is informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is in de AVG een wettelijk verankerde verplichting voor de bescherming van persoonsgegevens en kan om die reden niet los van elkaar worden gezien.
Voor de begripsbepalingen die in het beleid worden gehanteerd — zoals persoonsgegevens, verwerking, verwerkingsverantwoordelijke worden de definities gehanteerd overeenkomstig Artikel 4 van de AVG. (voor de leesbaarheid bevat bijlage 1 deze definities).

Doel
Met dit privacybeleid geeft de Gemeente Kerkrade een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen, waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid op hoofdlijn taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

Ambitieniveau Kerkrade
De gemeente werkt aan het vertrouwen van onze inwoners, bedrijven en belanghebbenden door aantoonbaar en blijvend te innoveren en investeren in privacy en informatieveiligheid. De gemeente voldoet aan de wettelijke verplichtingen voorkomend uit de AVG. De ambitie van de gemeente is om op de privacy borging volwassenheidsniveau 3 te bereiken en dit niveau daarna ook vast te houden. Het volwassenheidniveau 3 binnen het VNG-privacyborgingsproduct staat voor een beheerst niveau van privacy beheer. De organisatie heeft privacy structureel verankerd in beleid, processen en gedrag. Er is sprake van actieve sturing en monitoring, aantoonbare naleving van wet- en regelgeving (zoals de AVG), regelmatige evaluatie en verbetering en geborgde structurele bewustwording en training in organisatiecultuur. Bij het volwassenheidsniveau 3 is de privacy niet langer een losse verantwoordelijkheid, maar een integraal onderdeel van bedrijfsvoering.
De Gemeente Kerkrade volgt de landelijke ontwikkelingen en maakt waar mogelijk gebruik van de handreikingen van de Vereniging van Nederlandse Gemeenten (VNG). De Gemeente Kerkrade heeft niet de ambitie en ook niet de middelen om landelijk koploper te zijn bij het verder ontwikkelen van het landelijk privacy-instrumentarium.

Scope
Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:
a. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
b. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
c. De gegevensuitwisseling met derde partijen zoals samenwerkingsverbanden of externen.

Veruit de meeste verwerkingen van persoonsgegevens vallen onder de regels van de AVG/UAVG. Voor enkele specifieke gemeentelijke taken (strafrechtelijke opsporing en handhaving uitgevoerd door Boa's) is sprake van de uitvoering van een politietaak en is de Wet politiegegevens (Wpg) van toepassing. Specifieke kaders voor de verwerking van politiegegevens zijn opgenomen in het vastgestelde WPG beleid van de Gemeente Kerkrade.

Uitgangspunten
1 Het Privacy Control Framework vormt het bepalende kader voor de privacy-inrichting en beheersing binnen de gemeentelijke dienstverlening en bijbehorende processen.
2 De beleidsplannen Informatiebeleid, Informatiebeveiligingsbeleid een privacybeleid zijn integraal op elkaar afgestemd.
3 Het borgingsproduct van de VNG wordt als het beoordelingsinstrument gehanteerd voor het beoordelen van privacy compliance binnen de gemeente.
4 Iedereen werkzaam binnen of namens de gemeente Kerkrade is verantwoordelijk voor het verantwoord omgaan met en beschermen van persoonsgegevens.
5 Alle medewerkers en alle personen die werkzaam zijn voor de gemeente dragen actief de uitgangspunten en principes vastgelegd in dit privacybeleid uit.
6 Privacy "Awareness" is standaard onderdeel van trainingsprogramma's.
7 De gemeente Kerkrade past bij de ontwikkeling van nieuwe en bestaande diensten, systemen of processen de methodiek van Privacy by Design (PbyD) en Privacy by Default (PbyDF) toe. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.
8 De gemeente hanteert een risico gebaseerde aanpak. Dit houdt in dat de te treffen maatregelen altijd worden afgewogen tegen de risico's die met die maatregel worden gemitigeerd. Mitigerende maatregelen worden afgewogen tegen de inspanning, kosten en stand van de techniek.
9 De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen.
10 De gemeente heeft een effectieve organisatie- en rapportage-structuur om de privacy te borgen en te voldoen aan wet- en regelgeving.
11 Naast toezicht door de FG voert de gemeente op onderdelen specifieke privacy-audits uit.
12 Door structurele verbeteringen wil de gemeente de komende jaren de privacy bewustwording en de professionalisering van de privacy functies in de organisatie verhogen.
Randvoorwaarden
1 Dit privacybeleid is door het college van Burgemeester en Wethouders vastgesteld.
2 Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's) kan het college besluiten tot een tussentijdse herziening.
3 Een goede privacy borging is noodzakelijk voor het goed functioneren van de Gemeente Kerkrade en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.
4 De Gemeente Kerkrade beschouwt het onderhouden van adequate kennis op het gebied van privacy als goed werkgever- én goed werknemerschap. Structurele privacy bewustwording is randvoorwaardelijk.
5 In control zijn betekent dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er zowel gemeente breed als op afdelingsniveau een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.
6 Alle risico's afdekken is qua capaciteit en kosten niet mogelijk. Voor privacy vindt hiertoe jaarlijks een privacy risico-inschatting plaats op alle processen en worden (pre-)DPIA's uitgevoerd op alle processen met een hoog risico. Deze DPIA's worden periodiek herhaald.
7 De gemeente beschikt over een proceshuis waarin alle gestructureerde activiteiten die plaatsvinden onder de verantwoordelijkheid van de gemeente een plek hebben. Voor de processen waarin persoonsgegevens verwerkt worden is er een gedetailleerde procesbeschrijving beschikbaar. Dit geldt ook voor nieuwe diensten, voorafgaand aan de uitrol. De procesbeschrijving vormt de basis voor de toetsing van de privacy-borging in het proces (checklist privacy/DPIA) en het register van verwerkingen.
8 Het is van belang om direct bij het ontwikkelen van nieuwe en bestaande diensten, systemen of processen PbyD/PbyDF toe te passen.
9 Bij de uitwerking van het privacybeleid en bij de operationele uitvoering in de 1e (uitvoerende) en 2e (ondersteunende en adviserende) lijn wordt altijd vooraf gezorgd voor voldoende capaciteit. Dit is het leidend principe bij de toepassing en uitvoering van alle strategische principes voor verwerking van persoonsgegevens. De borging van privacy in de processen is een optelsom van de inspanningen van de privacy officers en de lijn gezamenlijk.
De gemeente staat voor grote financiële uitdagingen en moet keuzes maken tussen wat wenselijk is en wat haalbaar is qua capaciteit en middelen. Deze keuzes worden zorgvuldig afgewogen, vastgelegd en breed geaccepteerd binnen de organisatie, zodat duidelijk is waarom bepaalde zaken wel of niet worden opgepakt.

Toezicht en borging
Onder de verantwoordelijkheid van het college van B&W vindt een groot aantal verwerkingen van persoonsgegevens plaats. Op deze verwerkingen vindt extern en intern toezicht plaats. De FG ziet erop toe dat de AVG en intern wordt nageleefd. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. De gemeente is verplicht om een FG aan te stellen. De FG is intern toezichthouder, heeft een adviserende, informerende en toezichthoudende taak en een onafhankelijke positie in de organisatie. De FG van de gemeente is een aanspreekpunt voor privacy vragen van burgers.
De Gemeente Kerkrade past het borgingsproduct van de VNG als het beoordelingsinstrument voor het waarborgen van privacy compliance binnen de gemeente. Het borgingsproduct is een toetsingskader wat door de gemeente gebruikt wordt voor het duiden van privacy risico's en de daarbij behorende (nog te treffen) beheersmaatregelen binnen de gemeente.
De Functionaris Gegevensbescherming (FG) brengt jaarlijks een verslag uit aan het College van B&W (verwerkingsverantwoordelijke). In dit verslag rapporteert de FG over resultaten van het borgingsproduct, werkzaamheden, bevindingen en aanbevelingen over nog te nemen maatregelen.
De inrichting, sturing, meting en verbetering van dit privacybeleid vindt gestructureerd plaats volgens een duidelijke PDCA-cyclus (Plan-Do-Check-Act). En altijd langs dezelfde 5 'privacy-pijlers':
1 Beleidsvorming
2 Bewustwording
3 Privacy instrumenten
4 Beveiligen
5 Monitoren

De gemeente heeft een effectieve organisatie- en rapportage-structuur om de privacy te borgen en te voldoen aan wet- en regelgeving. De rapportage structuur stelt bestuurders en het management van de gemeente Kerkrade in staat om sturing te geven aan de governance en verdere implementatie van de AVG kaders.

Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal beginselen voor de verwerking van persoonsgegevens (artikel 5 AVG). Deze kernbegrippen zijn: rechtmatigheid, behoorlijkheid en transparantie (1.1), doelbinding (1.2), minimale gegevensverwerking (1.3), juistheid (1.4), opslagbeperking (1.5) en integriteit en vertrouwelijkheid (1.6) en beveiliging. De gemeente onderschrijft de AVG-beginselen en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze beginselen. Bij de inrichting van de processen hanteert de gemeente daarbij de onderstaande principes
1.1 Rechtmatigheid, behoorlijkheid en transparantie
Persoonsgegevens worden door de gemeente slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak. Afhankelijk van de verwerking kan daarnaast ook een van de andere verwerkingsgrondslagen worden toegepast zoals toestemming, uitvoering van een overeenkomst, vitaal belang en gerechtvaardigd belang. Deze laatste is enkel van toepassing op de medewerkers van de gemeente Kerkrade.
De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.
Hoe de gemeente omgaat met persoonsgegevens is opgenomen in de privacyverklaring op de website en de gepubliceerde gemeente register van verwerkingen (GRV). Meer specifiek worden betrokkenen geïnformeerd op het moment dat zij gegevens verstrekken, bijvoorbeeld door informatie op het aanvraagformulier, een flyer en/of specifieke info per onderwerp op de website.
1.2 Doelbinding en verdere verwerking
De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel dat aansluit op de wettelijke taken, mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente streeft om altijd op de minst ingrijpende wijze het doel te bereiken. In gevallen, waar mogelijk met geanonimiseerde of gepseudonomiseerde gegevens.
Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn en er zich geen nadelige effecten voor de betrokkenen voordoen. De gemeente voert,

voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.
De gemeente verstrekt nooit informatie aan andere inwoners of voor commerciële doeleinden. De gemeente verkoopt, verruilt of verhandelt persoonsgegevens nooit naar derden.

1.3 Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid

1.4 Juistheid

De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

1.5 Opslagbeperking

De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.
Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

1.6 Integriteit en vertrouwelijkheid

De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens (zoals bijvoorbeeld gezondheids- en strafrechtelijke gegevens, etnische afkomst of seksuele gerichtheid) te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. Het gemeentelijke informatiebeveiligingsbeleid beschrijft welke maatregelen hiertoe worden getroffen. Conform het intern toegangs- en autorisatiebeleid wordt informatie beveiligd tegen ongeautoriseerd gebruikt, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking. De externe digitale toepassingen worden gebruik indien de gegevens daar voldoende veilig zijn en de gemeente grip en zeggenschap heeft op het gebruik hiervan.

1.7 Doorgifte buiten de Europese Economische Ruimte

De gemeente verwerkt bij voorkeur geen persoonsgegevens buiten de Europese Economische Ruimte (EER). Uitgangspunt is dat verwerking buiten de EER alleen is toegestaan als er geen redelijke alternatieve oplossing binnen de EER beschikbaar is. Bij het inkooptraject wordt dit in de bestekfase meegenomen. Bij verwerking buiten de EER wordt voorafgaand risicoanalyse uitgevoerd. De privacy officer zal deze risicoanalyse uitvoeren en hierover altijd advies inwinnen bij de Functionaris Gegevensbescherming.

1.8 Artificiële Intelligentie, algoritmes en geautomatiseerde besluitvorming

De gemeente volgt de ontwikkelingen op het gebied van de algoritmische toepassingen, AI-systemen en vereisten uit de Europese AI-verordening (AI Act). Deze ontwikkelingen en toepassingen worden getoetst aan de AVG/ UAVG als hierbij persoonsgegevens verwerkt worden.
Om de wettelijke rechten van betrokkene te waarborgen treft de verwerkingsverantwoordelijke bij geautomatiseerde individuele besluitvorming passende maatregelen ter bescherming van deze rechten, vrijheden en gerechtvaardigde belangen. Hieronder vallen in ieder geval het recht op transparantie, het recht op menselijke tussenkomst, het recht om het eigen standpunt kenbaar te maken en het recht om het besluit aan te vechten. Het is wettelijk verplicht om op dergelijke verwerkingen een Data Protection Impact Assessment (DPIA) uit te voeren om de risico's voor betrokkenen te mitigeren.
In dit privacy beleid opgenomen principes voor het verwerken van de persoonsgegevens gelden onverminderd ook voor de verwerkingen van persoonsgegevens waarbij algoritmes en AI-systemen worden ingezet.

Privacy instrumenten

Register van verwerkingsactiviteiten

De Gemeente Kerkrade beschikt over een verwerkingsregister, zoals bedoeld in artikel 30 AVG waarin alle verwerkingen van persoonsgegevens gedocumenteerd en inzichtelijk zijn gemaakt. Het register van verwerkingen is een dynamisch document. De proceseigenaren dragen verantwoordelijkheid om het register periodiek, minimaal jaarlijks, te beoordelen op actualiteit en volledigheid. Het beheer van het register van verwerkingen is verder uitgewerkt in een protocol.

2.2 Gegevensbeschermingseffect beoordeling (GEB/DPIA)
Als een verwerking mogelijk een hoog privacy risico inhoudt voor betrokkenen of voorkomt op de verplichte lijst van GEB/DPIA's, voert de gemeente een Gegevensbeschermingseffectbeoordeling (GEB/Data Protection Impact Assessment/DPIA) uit op deze verwerking van persoonsgegevens. Om het privacy risico te bepalen hanteert de gemeente een Pre-DPIA, waarin een afwegingskader is opgenomen. Daarnaast volgt de gemeente de criteria van de Autoriteit Persoonsgegevens of een verwerking DPIA verplicht is *1. De privacy officer adviseert hierover aan de proceseigenaar.
In de gemeente voert een proceseigenaar een DPIA uit, waarbij de privacy officer ondersteunt. Iedere DPIA wordt conform de procesbeschrijving door de proceseigenaar voor advies voorgelegd aan de FG. Het advies wordt door de FG besproken met de betreffende proceseigenaar, die schriftelijk reageert op het advies van de FG. Indien het DPIA-verslag (met genomen maatregelen) volledig is en voldoet aan de eisen, wordt de DPIA door de proceseigenaar vastgesteld. Gelet op de mandaatregeling vindt er geen verdere communicatie plaats naar het college.
Indien niet kan worden voldaan aan de voorgestelde maatregelen en er aldus een hoog rest-risico blijft bestaan verzoekt de gemeente Kerkrade om een zogenaamde "voorafgaande raadpleging" bij de Autoriteit Persoonsgegevens.
De DPIA's worden periodiek herhaald. De frequentie is hierbij afhankelijk van het risico en de specifieke omstandigheden van het betreffende proces. Met een minimum frequentie van eens per 5 jaar.
*1 Besluit lijst verwerkingen persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens.

2.3 Overeenkomsten
De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Wanneer derden in opdracht van de gemeente werken, en de gemeente het doel en middelen van gegevensverwerking bepaald, worden deze derden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten. De gemeente maakt hiervoor gebruik van het, meest recente, sjabloon VNG verwerkersovereenkomst.
De gemeente schakelt soms ook derden in om in gezamenlijkheid, of volledig zelfstandig, persoonsgegevens te verwerken. Deze partijen zijn dan gezamenlijk verwerkingsverantwoordelijke óf zelfstandig verwerkingsverantwoordelijke. In dit geval wordt te allen tijde een gegevensleveringsovereenkomst overeengekomen.

2.4 Datalek melding en registratie
Bij oneigenlijke toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en bij de getroffen betrokkenen (er zijn enkele uitzonderingen). De gemeente registreert datalekken in het verplichte "datalekregister", zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. De afhandeling van datalekken geschied op basis van de Procedure datalekken. De procesverantwoordelijke werkt hierbij nauw samen met de Privacy – Officers, Information Security Officers (ISO) en vraagt desgewenst advies van de Functionaris Gegevensbescherming (FG).

2.5 Privacy by design en Privacy by Default
Door Privacy by Design (PbyD)/ privacy bij ontwerp en Privacy by Default (PbyDF) / privacy bij standaard instellingen toe te passen besteed de gemeente Kerkrade tijdens het ontwikkelen van producten, diensten en inrichten van informatiesystemen aandacht aan privacy verhogende maatregelen. Bij PbyD wordt er in een zo vroeg mogelijk stadium nagedacht over het gebruik van persoons- en politiegegevens binnen de organisatie, over de noodzaak van het gebruik van gegevens en over de bescherming ervan. Voorts zijn de standaardinstellingen (PbyDF) van een programma in de ontwerpfase altijd ingesteld op de meeste privacy vriendelijke manier. De keuze tot het verstrekken van meer informatie blijft bij de betrokkene.
De gemeente Kerkrade heeft voor het toepassen van PbyD en PbyDF een handleiding opgesteld.

2.6 Training en bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Veel digitale incidenten ontstaan door fouten of onwetendheid van medewerkers. Medewerkers die vakspecifieke wet- en regelgeving in relatie tot het verwerken van de persoonsgegevens kennen en weten hoe ze risico's kunnen herkennen, zijn beter in staat om fouten te voorkomen.
De gemeente Kerkrade vindt het daarom belangrijk om al tijdens de onboarding nieuwe medewerkers te informeren over het intern beleid en afspraken met betrekking tot het verwerken van de persoonsgegevens. Daarnaast wordt bewustzijn voortdurend aangescherpt door verplichte trainingen door middel van e-learning op het gebied van digitaal veilig werken en bewust omgaan met (persoons)gegevens. Onderdeel van het beleid zijn ook de regelmatig terugkerende bewustwordingscampagnes. Deze campagnes worden in afstemming met andere informatiebeveiligingscampagnes opgepakt.

2.7 Communicatie
Het privacybeleid is vastgesteld door het college van B&W van de gemeente Kerkrade en na de vaststelling gepubliceerd op overheid.nl. Daarnaast is het beleid voor alle medewerkers uit de organisatie

toegankelijk op Intranet. Alle wijzigingen in de bijbehorende protocollen en procedures worden via Intranet berichten gecommuniceerd met de organisatie en interne stakeholders.
De privacy officers (PO) participeren in diverse gremia en project overleggen zowel intern en extern. Er vinden structureel periodieke PO en PO/ISO overleggen plaats. Daarnaast zijn er afhankelijk van de onderwerpen periodieke overleggen met de CISO en FG.

Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. De gemeente heeft hiervoor een afhandelingsprocedure ingericht. De klachten inzake een persoonsgegevensverwerking wordet door de FG afgehandeld. Onderdeel van de afhandelingsprocedure is dat de gemeente te allen tijde de identiteit van de verzoeker dient vast te stellen. De gemeente biedt hierin de mogelijkheid voor digitale identificatie én identiteitsvaststelling in persoon.
Bij algemene inzageverzoeken, waarvan de vraagstelling niet duidelijk is, wordt vooraf contact gezocht met de aanvrager om te kijken of het verzoek kan worden verduidelijkt. Met als doel dat betrokkene een meer toegespitst besluit krijgt, dat beter antwoord geeft op de achterliggende vraag van betrokkene. Voor zover een verzoek geen betrekking heeft op persoonsgegevens kan deze op basis van artikel 6.30 Wet open overheid worden afgehandeld.

3.1 Geschillenbeslechting

Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.
Dergelijke klachten worden door de FG gecoördineerd.

3.2 Privacy Wet Open Overheid (WOO)

De gemeente heeft de intentie om open en transparant naar buiten te zijn, maar borgt gelijk ook de privacy van haar medewerkers en inwoners. Het gaat hierbij om de balans tussen het geven van optimale transparantie aan onze inwoners en organisaties en het beschermen van de privacy van betrokkenen. Er wordt rekening gehouden met belangen die openbaarmaking in de weg kunnen staan waarbij de AVG en de uitvoeringswet AVG leidend zijn voor wat betreft privacy. Zo worden alle naar personen te herleiden gegevens uit documenten onleesbaar gemaakt op een enkele uitzondering na: denk aan de naam van de burgemeester of degene die mandaat hebben om te ondertekenen.

Rollen en verantwoordelijkheden

Het governancemodel van de gemeente Kerkrade biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het College van B&W, de concerndirectie en medewerkers, de FG, PO, CISO en ISO.
Elk zelfstandig bestuursorgaan (ZBO) is verplicht om een eigen governance structuur en toezichthouder (FG) formeel te benoemen.

	Verantwoordelijk	
R	Responsible/ Feitelijk verantwoordelijk	• Proceseigenaren en Concerndirectie • De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable/ Eindverantwoordelijk	• Het college van B&W,
C	Consulted/ Adviserend	• Privacy Officer • CISO/ISO • Functionaris Gegevensbescherming
I	Informerend/ Geïnformeerd	• Gemeenteraad (privacy rechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

4.1 College van B&W

Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente.
Het College heeft de volgende rollen en verantwoordelijkheden:
a. Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente;
b. Stelt het privacybeleid vast;

c. Geeft sturing aan privacy-beleidsvoering en legt rekenschap af over privacy-beleidsvoering aan de FG;
d. Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
e. Stelt middelen beschikbaar om het privacybeleid te kunnen implementeren en borgen.

4.2 Proceseigenaren, afdelingshoofden, managementteam en concerndirectie

De gemeente stimuleert proceseigenaren in het voelen en nemen van verantwoordelijkheid en eigenaarschap voor de privacy en informatieveiligheid in hun processen. In de 1e lijn is voldoende capaciteit beschikbaar om de privacy in te regelen en te monitoren. Privacy is één van de taken die onderdeel uitmaken van het bredere procesmanagement/procesbeheer binnen de gemeente. Binnen de concerndirectie is de gemeentesecretaris eindverantwoordelijk voor de privacy-borging. De proceseigenaren/afdelingshoofden zijn verantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid.
De proceseigenaren hebben de volgende rollen en verantwoordelijkheden:
a. Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen processen en afdeling;
b. Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de processen en afdeling;
c. Verantwoordelijk voor het opstellen van domein specifieke privacy protocollen;
d. Informeert de FG op welke manier de eigen afdeling compliant is aan de privacywetgeving;
e. Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;
f. Verantwoordelijk voor het leveren van input op de inhoud van het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;
g. Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
h. Aansturen van de procesbeheerders binnen de eigen afdeling;
i. Bevordert duurzame privacy cultuur;
j. Betrekt PO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

4.3 Functionaris Gegevensbescherming (FG)

Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG werkt hierbij conform de 'FG regeling gemeente Kerkrade'.
Daarbij heeft de FG de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:
a. Interne toezichthouder op de naleving van de AVG namens de verwerkingsverantwoordelijke.
b. De contactpersoon voor de Autoriteit persoonsgegevens.
c. Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
d. Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
e. Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
f. Adviseert verwerkingsverantwoordelijken en PO bij privacy klachten en verzoeken van betrokkenen (ombudsfunctie);
g. Adviseert verwerkingsverantwoordelijken en PO ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
h. Adviseert bij de afhandeling van datalekken (volgens de meldprocedure);
i. Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
j. Rapporteert aan het College van B&W.

4.4 Privacy Officer (PO)

De Privacy Officer is het eerste aanspreekpunt voor de proceseigenaren rondom privacy gerelateerde vraagstukken, en heeft een coördinerende en controlerende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:
a. Participeert en adviseert bij de wijzigingen en projecten waarbij persoonsgegevens worden verwerkt.
b. Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
c. Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
d. Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
e. Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
f. Ondersteunt de verwerkingsverantwoordelijke bij het uitvoeren van DPIA's en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;

g. Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
h. Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
i. Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
j. Adviseert over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
k. Adviseert over de ontwikkeling van de bewustmakingsprogramma's- en privacy trainingen voor medewerkers en biedt ondersteuning bij het organiseren en uitvoeren van deze trainingen;
l. Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de ISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
m. Ondersteunt en adviseert bij de afhandeling van datalekken (volgens de meldprocedure) en zorgt voor een volledige en actuele datalek registratie;
n. Ondersteunt bij de afhandeling rechten van betrokkenen en bezwaar- en beroepsprocedures (met ondersteuning van proceseigenaar) inzake de verwerkingen van persoonsgegevens.
o. Op basis van de controlerende taken rapporteert PO aan procesverantwoordelijke en FG.
p. Toetst de compliancy van de verwerkingen van persoonsgegevens aan de AVG/UAVG en of deze verwerkingen in overeenstemming zijn met de algemene en bijzondere wetten waarop de taken en uitvoering zijn gebaseerd.

4.5 Overige stakeholders in de organisatie

De gegevensbescherming is een belangrijk onderdeel van elk proces in de gehele organisatie en vereist de samenwerking van alle belanghebbende. Alleen door gezamenlijk verantwoordelijkheid te nemen, kan een organisatie voldoen aan wet- en regelgeving zoals de AVG, en tegelijkertijd vertrouwen opbouwen bij burgers en medewerkers.
Belangrijke belanghebbende in gegevensbescherming zijn naast het college van B&W, directie, managementteam, proceseigenaren, FG en PO:
Raadsleden: Houden toezicht om de naleving van wet- en regelgeving door de verwerkingsverantwoordelijke college van B&W.
Portefeuillehouder privacy: Is vanuit het college belast met sturing op gegevensbescherming.
(C) ISO: Adviseert en beheert beveiligingsmaatregelen conform Baseline informatiebeveiliging overheid (BIO) normering. Werkt samen met de PO's bij de afhandeling van de datalekken.
HR-afdeling: Verantwoordelijk voor het naleven van gegevensbescherming in personeelsadministratie, interne processen, onboarding, bewustwording en trainingen.
Juridische afdeling: Adviseert over de rechtmatigheid en de risico's. Ondersteunt en adviseert bij inkoop en aanbestedingsproces en betrekt PO's bij het proces.
Communicatie: Adviseert over de communicatie van het beleid en procedures binnen de organisatie.
Informatiemanagers en functioneel beheerders: Zorgen dat bij alle wijzigingen waarbij de persoonsgegevens betrokken zijn getoetst worden door de PO.
Medewerkers: Iedereen binnen de organisatie speelt een rol door bewust om te gaan met gevoelige informatie.
Leveranciers en samenwerkingspartijen: Dienen te voldoen aan de afspraken en normen van de organisatie omtrent gegevensbescherming.
Samenwerking tussen alle afdelingen en belanghebbenden zorgt ervoor dat gegevensbescherming niet slechts een taak is van de afdeling Informatie, maar een gedeelde verantwoordelijkheid die de organisatie als geheel sterker en veiliger maakt.

Aldus vastgesteld door het college van burgemeester en wethouders van Kerkrade in zijn vergadering van 03 februari 2026
Het college, de secretaris,
dr. T.P. Dassen-Housen R.M.J.S Stijns

Bijlage 1 Definities artikel 4 AVG

Voor de toepassing van deze verordening wordt verstaan onder:

1) „persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); 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,s psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

2) „verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

3) „beperken van de verwerking": het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken;

4) „profilering": elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

5) „pseudonimisering": het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

6) „bestand": elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

7) „verwerkingsverantwoordelijke": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

8) „verwerker": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat namens de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

9) „ontvanger": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;

10) „derde": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;

11) „toestemming" van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt;

12) „inbreuk in verband met persoonsgegevens": 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 gegevens; (NB. Niet opgeloste vertaalfout. Lees i.p.v. 'ongeoorloofde': 'onbevoegde'. Zie Engels: unauthorised; Duits: unbefugten; Frans: non-autorisée, JT).

13) „genetische gegevens": persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;

14) „biometrische gegevens": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;

15) „gegevens over gezondheid": persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

16) „hoofdvestiging": a) met betrekking tot een verwerkingsverantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslis-

singen over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd;
b) met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten;
17) „vertegenwoordiger”: een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;
18) „onderneming”: een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;
19) „concern”: een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend;
20) „bindende bedrijfsvoorschriften”: beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meer derde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen;
21) „toezichthoudende autoriteit”: een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie;
22) „betrokken toezichthoudende autoriteit”: een toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens omdat:
a) de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd;
b) de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of
c) bij die toezichthoudende autoriteit een klacht is ingediend;
23) „grensoverschrijdende verwerking”:
a) verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of
b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden;
24) „relevant en gemotiveerd bezwaar”: een bezwaar tegen een ontwerpbesluit over het bestaan van een inbreuk op deze verordening of over de vraag of de voorgenomen maatregel met betrekking tot de verwerkingsverantwoordelijke of de verwerker strookt met deze verordening, waarin duidelijk de omvang wordt aangetoond van de risico's die het ontwerpbesluit inhoudt voor de grondrechten en de fundamentele vrijheden van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie;
25) „dienst van de informatiemaatschappij”: een dienst als gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad (19);
26) „internationale organisatie”: een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.