PRIVACY

Functieprofiel Functionaris Gegevensbescherming

BMGRIP

BMGRIP

Alles over de AVG gids

Inhoudsopgave

1. Doel van de functie

De Algemene Verordening Gegevensbescherming (AVG) biedt een gemoderniseerd, op verantwoording gebaseerd kader voor de naleving van regels inzake gegevensbescherming in Europa. Functionarissen voor gegevensbescherming zullen in dit nieuwe juridische kader voor veel organisaties centraal staan om naleving van de bepalingen van de algemene verordening gegevensbescherming mogelijk te maken.

De functionaris voor de gegevensbescherming (FG) speelt een fundamentele rol in het creëren van een cultuur van gegevensbescherming binnen de organisatie en helpt ook bij de implementatie van essentiële elementen uit de AVG, zoals de beginselen van gegevensverwerking, de rechten van de betrokkenen, gegevensbescherming door ontwerp en gegevensbescherming door standaard-instellingen, register van verwerkingsactiviteiten, beveiliging van de verwerking en melding van en communicatie over inbreuken met betrekking tot gegevens.

2. Plaats in de organisatie

De FG is betrokken bij alle kwesties met betrekking tot het beschermen van persoonsgegevens. De FG moet op een juiste en tijdige manier betrokken worden door zowel de verwerker als de verwerkingsverantwoordelijke van persoonsgegevens. Specifiek bij het uitvoeren van de Data Protection Impact Assessment (DPIA) dient de FG in het vroegste stadium te worden betrokken. Hierbij dienen de verwerker en de verwerkingsverantwoordelijke advies te vragen aan de FG. Door de FG al vanaf het startpunt te betrekken bij alle zaken rondom gegevensbescherming wordt het gemakkelijker om te voldoen aan de wet- en regelgeving en wordt het privacy by design-principe nageleefd. De FG dient als discussiepartner te worden gezien en hij/zij zal deel moeten nemen aan relevante werkgroepen die persoonsgegevens verwerken in hun werkzaamheden.

Dit betekent dat:

- De FG regelmatig wordt uitgenodigd om vergaderingen van het hogere management en het middenkader bij te wonen;
- Zijn/haar aanwezigheid wordt aanbevolen wanneer beslissingen worden genomen die gevolgen hebben voor de gegevensbescherming. Alle relevante informatie moet tijdig aan de FG worden bezorgd, zodat hij/zij passend advies kan verlenen;
- De mening van de FG naar behoren in overweging wordt genomen. Bij onenigheid is het aan te raden om de redenen voor het niet volgen van het advies van de FG tdocumenteren;
- De FG meteen wordt geconsulteerd zodra zich een gegevensinbreuk of een ander incident voordoet.
- De organisatie dient de FG die benodigde middelen te geven die hij/zij nodig heeft om zijn/haar taken te voldoen, toegang te geven tot de persoonsgegevens en operationele processen, en de tijd en ruimte om zijn expertise met betrekking tot het beveiligen van persoonsgegevens op peil te houden.

Hierbij kunnen de volgende zaken worden overwogen:

- Actieve ondersteuning van de functie van FG door het hogere management (zoals op niveau van de raad van bestuur).
- Voldoende tijd voor de FG om de taken te vervullen. Dit is vooral belangrijk wanneer een interne FG op deeltijdse basis is aangesteld of wanneer de externe FG naast zijn andere taken ook voor gegevensbescherming instaat.
- Adequate ondersteuning op het vlak van financiële middelen, infrastructuur (kantoren, faciliteiten, apparatuur) en personeel waar van toepassing.
- Officiële bekendmaking van de aanstelling van de FG aan alle personeelsleden om te verzekeren dat iedereen in de organisatie op de hoogte is van het bestaan van deze functie.
- Noodzakelijke toegang tot andere diensten zoals HR, juridische dienst, IT, beveiliging enz., zodat de functionarissen voor gegevens-bescherming van die andere diensten de benodigde essentiële ondersteuning, bijstand of informatie kunnen ontvangen.
- Voortgezette opleiding. De FG moet de kans krijgen om op de hoogte te blijven van nieuwe ontwikkelingen op het vlak van gegevensbescherming. Daarbij moet het de bedoeling zijn het niveau van de deskundigheid van de FG permanent te verhogen en hen aan te moedigen deel te nemen aan opleidingen over gegevensbescherming en aan andere vormen van professionele ontplooiing, zoals deelname aan fora over privacy, workshops enz.
- Gezien de grootte en structuur van de organisatie kan het nodig zijn om een team rond de FG samen te stellen (een FG en zijn/haar personeelsleden). In die gevallen moeten de interne structuur van het team en de taken en verantwoordelijkheden van ieder lid duidelijk worden vastgelegd. Wanneer de functie van FG door een externe dienstverlener wordt bekleed, kan op dezelfde manier een team van personen die voor die entiteit werken feitelijk alle taken van de FG als team uitvoeren, onder de verantwoordelijkheid van een aangestelde hoofdcontactpersoon van de klant.

- Het is van belang dat de FG autonoom kan handelen binnen de organisatie. De FG dient dus in de positie te worden gesteld dat hij/zij de benodigde taken zelfstandig en onafhankelijk uit kan voeren, zonder dat er door anderen stringente instructies worden opgelegd. De verwerkingsverantwoordelijke en verwerker van de persoonsgegevens blijft echter wel verantwoordelijk voor de uitvoering en moet aan kunnen tonen dat dit volgens de wet- en regelgeving gebeurt.

3. Resultaatgebieden

Beleid en coördinatie

- Het opstellen en actualiseren van het beleid inzake het verwerken van persoonsgegevens (langere termijn).
- Het coördineren van de werkzaamheden rondom het verwerken van persoonsgegevens.

Controle en registratie

- Het toezicht houden op de implementatie en naleving van het op de juiste manier verwerken van persoonsgegevens (o.a. principes als: privacy by design en privacy by default).
- Het opstellen van een controleplan, evenals het leveren van ondersteuning bij het uitvoeren van de daarin gedefinieerde taken.
- Het opstellen of initiëren en actualiseren van een stakeholdersanalyse.
- Het opstellen of initiëren van een gedragscode voor personeelsleden van de organisatie.
- Het opstellen of initiëren van een geheimhoudingsverklaring voor personeelsleden van de organisatie.
- Indien nodig, het uitvoeren of initiëren van een DPIA.
- Het opstellen of initiëren van een verwerkingsregister persoonsgegevens.
- Het opstellen of initiëren en publiceren van een privacyverklaring.

- Indien nodig, het opstellen of initiëren en implementeren van verwerkings-overeenkomsten met stakeholders.
- Het verzamelen en registreren van informatie over de aanwezige manieren van verwerken van persoonsgegevens.
- Het opzetten of initiëren van een registratie voor incidenten rondom het verwerken van persoonsgegevens, evenals het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten (melden datalekken).

Communicatie en voorlichting

- Het onderhouden van externe en interne contacten op alle niveaus binnen dit kader.
- Het organiseren van overleg met betrekking tot het verwerken van persoonsgegevens.
- Het verzorgen en coördineren van voorlichting en interne opleidingen van het (toekomstig) personeel op het gebied van het verwerken van persoonsgegevens.
- Het stimuleren van het bewustzijn omtrent het verwerken van persoonsgegevens bij het opstellen, uitvoeren en onderhouden van een communicatieplan.
- Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van verwerking van persoonsgegevens.

Advies en rapportage

- Het uitwerken van plannen inzake het verwerken van persoonsgegevens ten aanzien van de maatregelen, evenals het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen.
- Het geven van gevraagd en ongevraagd advies aan de stakeholders over de te nemen maatregelen.
- Het rapporteren aan de stakeholders over het gevoerde beleid met betrekking tot het verwerken van persoons-gegevens, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onder-zoeken en resultaten van controles.

4. Taken, verantwoordelijkheden en bevoegdheden

De FG is in eerste instantie verantwoordelijk voor het monitoren van de mate van overeenstemming met de AVG.

Hieronder valt onder andere:

- Informatie verzamelen om verwerkingsactiviteiten te identificeren;
- De naleving van verwerkingsactiviteiten analyseren en controleren;
- De verwerkingsverantwoordelijke of de verwerker informeren, adviseren en aanbevelingen doen.
  Indien er een afwijking of niet conformiteit aan de AVG plaatsvindt is de FG niet verantwoordelijk Het is de verantwoordelijkheid van de verwerkings-verantwoordelijke om passende technische en organisatorische maatregelen te nemen om te waarborgen en te kunnen aantonen dat het proces wordt uitgevoerd in conformiteit met de AVG. Het uitvoeren van een DPIA is de verantwoordelijkheid van de verwerkingsverantwoordelijke. De FG kan hierbij echter een belangrijke rol spelen, daar hij om advies dient te worden gevraagd bij het uitvoeren hiervan. Hier dient de FG gehoor aan te geven. De FG wordt om advies gevraagd inzake onder andere onderstaande punten:
- Of er al dan niet een DPIA moet worden uitgevoerd;
- Welke methodologie bij een DPIA moet worden gevolgd;
- Of de DPIA intern uitgevoerd of uitbesteed moet worden;
- Welke waarborgen (waaronder technische en organisatorische maatregelen) moeten worden toegepast om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
- Of de DPIA al dan niet correct is uitgevoerd en of de conclusies (de verwerking al dan niet uitvoeren en welke waarborgen toepassen) al dan niet in overeenstemming zijn met de algemene verordening gegevensbescherming;

- De FG dient te allen tijde het risico dat gepaard gaat met het verwerken van persoonsgegevens in de verschillende bedrijfsprocessen in ogenschouw te nemen. Hierbij kan er een ordening worden gemaakt waarbij zaken met een hoger risicoprofiel prioriteit krijgen.
- Hoewel het de verantwoordelijkheid is van de verwerkings verantwoordelijke of de verwerker van persoonsgegevens om een archief inzake diens processen bij te houden, komt het in de praktijk vaker voor dat de FG deze archieven aanmaakt en bijhoudt. Deze archieven worden gevuld met informatie afkomstig van verschillende afdelingen binnen het bedrijf die persoonsgegevens verwerken. Een dergelijk archief kan als middel worden gezien om de conformiteit aan de AVG te monitoren, maar kan tevens als basis dienen bij het adviseren van verwerkingsverantwoordelijke en verwerker. Daarnaast biedt het een overzicht van alle persoonsgegevens die worden verwerkt binnen de organisatie (Verwerkingsregister persoonsgegevens);
- Als laatste dient de FG mee te werken met de toezicht houdende autoriteit en als contactpersoon hiervoor te dienen inzake de verwerking maar ook de voorgaande contacten met de toezichthoudende autoriteit.

5. Contacten

De FG dient zowel intern als extern contact te onderhouden met relevante stakeholders. De FG dient daarbij zorg te dragen voor het structureren van vaste en ad-hoc overlegvormen. Extern contact is er met toezichthouders, service providers en (indien relevant) politie/justitie. Extern wisselt de FG kennis en ervaring uit met vakgenoten. Om op de hoogte te blijven van nieuwe ontwikkelingen is contact met leveranciers (beurzen, lidmaatschap gebruikersgroepen van bepaalde producten) tevens van belang.

6. Opleiding, kennis, ervaring en competenties

De FG wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de bedoelde taken te vervullen. Het niveau van deskundigheid van de FG moet in verhouding zijn tot de gevoeligheid alsmede de complexiteit van de gegevens, maar ook de hoeveelheid gegevens die een organisatie verwerkt.

Voor wat betreft de professionele kwaliteiten dient te worden gekeken naar de ervaringen die de functionaris heeft op het gebied van nationale en Europese wetten en praktijken omtrent gegevensbescherming. Daarnaast is de kennis over de AVG een relevant element. Daarnaast is het nuttig als de functionaris voldoende kennis heeft van de bedrijfstak en van de organisatie van de verwerkingsverantwoordelijke. Ook dient de functionaris voldoende inzicht hebben in de uitgevoerde verwerkingsactiviteiten, de informatiesystemen en de behoeften van de verwerkingsverantwoordelijke op het gebied van gegevensbeveiliging en gegevens-bescherming. Belangrijke persoonlijke kwaliteiten van de functionaris zijn bijvoorbeeld integriteit en een hoge mate van professionele ethiek.

De onderstaande punten mogen worden verwacht van de functionaris:

- Bovengemiddelde vakkennis van privacywetgeving en van de praktijk van gegevens-bescherming:
- Kennis van nationale en Europese privacywet- en regelgeving over gegevens-bescherming;
- Begrip van gegevensverwerkingen die de organisatie uitvoert;
- Begrip van IT en informatiebeveiliging;
- Kennis van de organisatie en de sector waarin die actief is;
- Vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.

BMGRIP
Computerweg 22
3542 DR Utrecht
030 - 755 53 55

info@bmgrip.nl,
www.bmgrip.nl

Versie juni 2022