NGFG
NEDERLANDS GENOOTSCHAP
FUNCTIONARISSEN GEGEVENSBESCHERMING

Een functionaris voor gegevensbescherming aanwijzen: val ik in de prijzen?

Waarover gaat deze brochure en voor wie is zij bestemd?

Ben ik verplicht om iemand aan te stellen als functionaris voor gegevensbescherming (FG)? En zo nee, kan een FG dan toch nuttig zijn? Voor het management van een organisatie zijn dit vaak lastige vragen. Deze brochure gaat over de vraag of het voor uw organisatie verstandig is om een FG aan te wijzen.

Inhoud

Wat is een functionaris voor gegevensbescherming (FG)?

Om deel te nemen aan het maatschappelijk verkeer is het noodzakelijk dat persoonsgegevens worden gebruikt. Zo heeft een bank persoonsgegevens nodig om bankrekeningen te kunnen beheren, een verzekeringsmaatschappij om een polisadministratie bij te kunnen houden, een sportvereniging om contributies te kunnen innen, een arts om een goede behandeling voor te kunnen stellen, en een gemeente om een vergunning te kunnen afgeven. Het is belangrijk dat persoonsgegevens op een zorgvuldige wijze worden verwerkt. Er zijn Europese en nationale regels die spelregels bevatten over de bescherming van personen bij het gebruik van hun gegevens. Die spelregels zijn onmisbaar in onze huidige samenleving. De belangrijkste staan in de Algemene verordening gegevensbescherming, oftewel: de AVG.

Een *functionaris voor gegevensbescherming* houdt binnen een organisatie toezicht op de naleving van privacyregels. Zo'n functionaris wordt aangewezen door het management en heeft ook een adviesfunctie. Een FG helpt zijn organisatie om risico's rondom de verwerking van persoonsgegevens inzichtelijk te maken, de regels na te leven en schade te voorkomen.

Wanneer is een FG verplicht?

U bent verplicht een FG aan te wijzen als uw organisatie behoort tot één van de volgende categorieën:

- Overheidsinstanties en publieke organisaties. Overheidsorganisaties zijn altijd verplicht een FG aan te wijzen. Het gaat hierbij om de rijksoverheid, gemeenten, en provincies. Maar ook zorg- en onderwijsinstellingen moeten een FG aanwijzen. Voor rechtbanken geldt de verplichting een FG aan te wijzen niet.
- Organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen, of hun activiteiten in kaart brengen. Het kan hierbij gaan om profilering van mensen voor het maken van risico-inschattingen, cameratoezicht, of monitoring van iemands gezondheid via bijvoorbeeld *wearables*. Relevant hierbij is onder meer het aantal mensen dat door een organisatie wordt gevolgd, hoelang dat gebeurt, en hoeveel gegevens de organisatie verwerkt.
- Organisaties die op ***grote schaal*** bijzondere persoonsgegevens verwerken wanneer dit voor hen een kernactiviteit is. Ziekenhuizen, zorggroepen, apotheken (niet zijnde 'solistisch' werkende zorgverleners) en huisartsenposten zijn dus verplicht een FG aan te stellen. Huisartsenpraktijken en andere instellingen voor medisch (specialistische) zorg verwerken gegevens op grote schaal als zij meer dan **10.000** ingeschreven patiënten hebben **óf** gemiddeld meer dan 10.000 patiënten per jaar behandelen.

Het privacyprofiel van uw organisatie

Ook wanneer een FG niet verplicht is, kan het een goed idee zijn een FG te benoemen. Of dat zo is, hangt af van verschillende factoren. Leidend is de vraag hoe hoog het privacyrisico is voor uw organisatie. De risico's die gepaard gaan met de verwerking van persoonsgegevens verschillen immers per organisatie. Ook de mate waarin het bestuur de risico's acceptabel vindt, speelt een rol. Dit kan ook per organisatie verschillen. Via de vragenlijst hieronder kunt u snel inzicht krijgen of het zinvol is om een FG aan te wijzen. De lijst wordt gevolgd door een toelichting bij de vragen, en vervolgens door de conclusie of voor uw organisatie een FG zou moeten worden aangewezen.

Vragenlijst privacy risicoprofiel

	Nee		Ja
Activiteiten van de organisatie 1. De kernactiviteiten zijn gericht op de verwerking van persoonsgegevens; *(zie de toelichting op blz. 4)*	groen	oranje	rood
Verkrijging van de gegevens 2. Betrokkenen zijn *(juridisch of feitelijk)* verplicht om hun gegevens af te staan en/of door uw organisatie te laten verwerken;	groen	oranje	rood *J
Hoeveelheid gegevens 3. De databases van uw organisatie bevatten persoonsgegevens over heel veel personen; *(< 1000= groen, 1000 – 10.000= oranje, > 10.000= rood. Het gaat hierbij om zowel werknemers als klanten)*	groen	oranje	rood
Hoog-risico verwerkingen 4.Uw organisatie is hoofdzakelijk belast met (grootschalige) gegevensverwerkingen met “hoog risico” als bedoeld in de AVG. Zie hiervoor ook de lijst van de Autoriteit persoonsgegevens; *(zie de toelichting op blz. 4)*	groen	oranje	rood
Complexiteit van de verwerkingen 5. Er is behalve de AVG, ook bijzondere (sectorale) wet- of regelgeving van toepassing op de verwerking van persoonsgegevens; *(bijvoorbeeld specifieke wetten, besluiten, gedragscodes)*	groen	oranje	rood *J
6. Er worden voor veel verschillende doeleinden gegevens geregistreerd en gebruikt of er zijn veel verschillende bestanden in de organisatie aanwezig, er zijn veel gebruikers/beheerders of er vinden veel uitwisselingen plaats met andere delen van de organisatie, of met derden zoals dienstverleners;	groen	oranje	rood *J
Verstrekking aan derden 7. Aan meer dan 10 (overheids)instanties worden gegevens verstrekt, of er worden gegevens verstrekt aan één of meer buitenlandse autoriteiten;	groen	oranje	rood *J
8. Er worden geregeld gegevens verstrekt aan een of meer derden die gevestigd zijn in landen buiten de EU;	groen	oranje	rood *J
Vragen over gegevensgebruik 9. In uw organisatie of bij uw klanten rijzen vaak vragen over wat er wel of niet mag met persoonsgegevens;	groen	oranje	rood *J
10. Er is behoefte aan 1 verantwoordelijk aanspreekpunt voor vragen over de verwerking van persoonsgegevens;	groen	oranje	rood *J
Complexiteit van de organisatie. 11. De organisatie heeft een complexe organisatiestructuur met veel verschillende afdelingen, meerdere divisies of vestigingen, of zij is gevestigd in meerdere landen;	groen	oranje	rood
Ambitie 12. Uw organisatie hecht grote waarde aan naleving van wet- en regelgeving, aan maatschappelijk zorgvuldig optreden of aan kwaliteit op het gebied van de informatievoorziening. Het is van wezenlijk belang dat uw organisatie vertrouwen geniet op het gebied van rechtmatigheid, zorgvuldigheid en kwaliteit, in het bijzonder wat betreft de verwerking van persoonsgegevens.	groen	oranje	rood
	aantal groen x 0 punten = 0 punten	aantal oranje x 1 punt = …… punten	aantal rood x 2 punten = …… punten
Totaal aantal punten		☐	…… ____ + …… (Totaal)

Toelichting bij de vragenlijst

Doel en inhoud van de vragenlijst
De vragen zijn bedoeld om er achter te komen of er sprake is van een “hoog privacy risicoprofiel” bij een organisatie. De vragen gaan dus niet over de vraag of de privacywetgeving AVG überhaupt wel van toepassing is. Dat is het geval als er sprake is van het verwerken van persoonsgegevens.

Door wie wordt de vragenlijst ingevuld?
Voor het invullen van de vragenlijst kan het nodig zijn verschillende disciplines en/of deskundigen te raadplegen. Denk in het bijzonder aan deskundigen op het gebied van de primaire bedrijfsprocessen, de gegevensverwerking, als aan de hogere manager en de bedrijfsjurist.

In geval van een concern
Voor grote, complexe organisaties (zoals multinationals en grote overheidsorganisaties) is het beter om de vragenlijst per business unit, divisie, directie of dienst in te vullen. De resultaten hebben dan betrekking op dat dienst- of bedrijfsonderdeel. De privacyfunctie moet namelijk worden afgestemd op de structuur en grootte van de organisatie. Het is dan van belang te weten bij welke organisatie-onderdelen accenten moeten worden gelegd. Er zullen in grote, complexe organisaties vaak één of meer decentrale privacyfunctionarissen nodig zijn.

Wat zijn “persoonsgegevens”?
Persoonsgegevens zijn alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. De meest sprekende voorbeelden zijn naam, adres of geslacht. Maar ook andere gegevens vallen onder de definitie van persoonsgegevens. Bijvoorbeeld gegevens die een waardering over iemand geven, zoals het resultaat van een onderzoek. Zelfs gegevens over ondernemingen of organisaties, of gegevens over voorwerpen of objecten, kunnen wel persoonsgegevens zijn. Dat is het geval als zij mede bepalend zijn voor de wijze waarop iemand in het maatschappelijk verkeer wordt beoordeeld of behandeld. Als u dan een verband kunt leggen tussen de informatie en een bepaalde natuurlijke persoon, is er sprake van een persoonsgegeven. De AVG is van toepassing op persoonsgegevens die worden verwerkt in het kader van de primaire taken (klantenadministratie, externe relaties, e.d.), maar ook op persoonsgegevens van het eigen personeel.

“Hoog-risico verwerking”
Er is op basis van de AVG sprake van “hoog risico” in de volgende gevallen:
- een systematische en uitgebreide beoordeling van persoonlijke aspecten gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd die gevolgen hebben voor mensen;
- op grote schaal verwerken van bijzondere (lees: gevoelige) persoonsgegevens;
- op grote schaal en stelselmatig volgen van mensen in een publiek toegankelijk gebied.

De Autoriteit Persoonsgegevens heeft daarnaast een lijst opgesteld van soorten hoog-risico verwerkingen. Deze lijst is niet uitputtend.

1. Heimelijk onderzoek 2. Zwarte lijsten 3. Fraudebestrijding 4. Creditscores 5. Financiële situatie 6. Genetische persoonsgegevens 7. Gezondheidsgegevens 8. Samenwerkingsverbanden 9. Cameratoezicht	10. Flexibel cameratoezicht 11. Controle werknemers 12. Locatiegegevens 13. Communicatiegegevens 14. Internet of things 15. Profilering 16. Monitoring en beïnvloeding van gedrag 17. Biometrische gegevens

Voor “hoog risico” moet in de meeste gevallen wel sprake zijn van “verwerking op grote schaal”. Er gelden de volgende criteria:
- het aantal betrokkenen (de mensen van wie u gegevens verwerkt);
- de hoeveelheid gegevens die u verwerkt;
- de duur van de gegevensverwerking;
- de geografische reikwijdte van de verwerking.

Zie voor meer informatie: https://autoriteitpersoonsgegevens.nl.

Conclusie: valt uw organisatie “in de prijzen?”

Door het aantal punten en het aantal rode scores op te tellen, kunt u het privacy-risicoprofiel van uw organisatie berekenen:

0 rood **9 punten of minder**	**1 x rood** **9 - 15 punten**	**>1 x rood** **Meer dan 15 punten**
Uw organisatie heeft geen bovengemiddeld privacy risico. U heeft de mogelijkheid een FG aan te wijzen.	Privacy is een onmiskenbare risicofactor in uw organisatie. Het verdient aanbeveling een FG aan te wijzen.	Privacywetgeving vormt een wezenlijk aandachtsgebied en risico. Het wordt sterk aanbevolen om een FG aan te wijzen.

Capaciteit en deskundigheid van de FG

Als u een FG gaat aanwijzen, moet u letten op het juiste functieprofiel en de kennis waarover de FG moet beschikken. Ook hierbij helpt de vragenlijst. De vuistregel is: hoe hoger de puntenscore, hoe hoger de deskundigheid en/of capaciteit van de FG moet zijn. Voor de capaciteit geldt daarnaast het volgende.

0 - 4 x groen	**> 4 x groen**
1 fulltimer (fte) of meer	Parttime is optie

De achtergrond van de FG is ook van belang. Uiteraard dient hij of zij altijd kennis van de privacywetgeving te hebben. Maar soms is er reden om deze juridische deskundigheid extra goed te borgen. De vragenlijst bevat antwoorden die gemarkeerd zijn met een “j”.

0 - 3 x "*J”	**> 3 x "*J”**
Juridisch of anders	Juridisch

De achtergrond van de FG kan bijvoorbeeld zijn: jurist, IT-specialist, auditor, of informatiebeveiligings-specialist.

Positionering

Wil de functionaris effectief kunnen functioneren, dan moet hij ook op de juiste positie in de organisatiestructuur worden geplaatst. Bijzonder aan de functie is, dat de FG zijn taken in onafhankelijkheid moet kunnen uitvoeren, en dat hij rapporteert aan de hoogste leiding. Dat is zo in de AVG bepaald. Het gaat er om dat de functionaris voldoende invloed kan uitoefenen om zijn belangrijke taak effectief te vervullen. Bij de positionering van de FG in de organisatie moet daar rekening mee worden gehouden.

De AVG

De AVG bevat normen voor het gebruik van persoonsgegevens. De belangrijkste beginselen zijn:

1. Doelbinding
Persoonsgegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en niet verder worden verwerkt voor doeleinden die daarmee onverenigbaar zijn.

2. Rechtmatigheid, behoorlijkheid en transparantie
Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Voor elk gebruik van persoonsgegevens moet een rechtmatige grondslag in de AVG te vinden zijn. Deze grondslagen zijn: ondubbelzinnige toestemming van de betrokkene of noodzakelijk voor de uitvoering van een overeenkomst, nakoming van een wettelijke plicht, de bescherming van een vitaal belang, voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dan wel een gerechtvaardigd belang van de organisatie of van een derde.

3. Minimale gegevensverwerking
De persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

4. Juist zijn en zo nodig worden geactualiseerd
Er moeten redelijke maatregelen zijn genomen om de gegevens te controleren op juistheid en de noodzaak deze gegevens te verwerken met het oog op doeleinden van de verwerking. Indien nodig worden gegevens verwijderd of verbeterd.

5. Opslagbeperking
De opgeslagen gegevens mogen niet langer bewaard worden dan noodzakelijk is.

6. Integriteit en vertrouwelijkheid
Door het nemen van passende technische en organisatorische maatregelen is een passende beveiliging gewaarborgd en zijn de gegevens beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen verlies, vernietiging of beschadiging.

7. Verantwoordingsplicht
De verwerkingsverantwoordelijk is verantwoordelijk voor de naleving van de AVG en kan aantonen dat hij dat doet.

Zie voor meer informatie over de AVG: https://autoriteitpersoonsgegevens.nl

De rol van de FG

Het is van belang dat een organisatie de nodige maatregelen treft in het kader van de AVG. De FG speelt een belangrijke rol bij het toezicht op en het adviseren over de verplichtingen van de AVG.

- **Het aanstellen van een FG is een passende maatregel wanneer privacyrisico's serieus worden genomen**
- **De FG helpt de naleving binnen de organisatie te bevorderen en de risico's te verkleinen**
- **De FG kent de gegevensverwerkingen en de organisatie, en kan daarom meedenken over passende oplossingen**
- **De FG is een vast aanspreekpunt en heeft een stevige adviesfunctie**
- **De FG kan de AP raadplegen**
- **De FG kan optreden als bemiddelaar of klachtenbehandelaar**
- **De FG bevordert het privacybewustzijn binnen de organisatie**
- **De FG draagt bij aan de betrouwbaarheid van zijn organisatie**

Ga voor meer informatie naar de website www.ngfg.nl.