Hoe ben je FG?
Handreiking voor de praktijk

Sergej Katus

Met dank aan:
Rob Hartgers voor het meeschrijven, en Maurice Reedijk en Koen Versmissen voor hun waardevolle commentaar.

Wolters Kluwer
Deventer 2020

Inhoud

Begrippenlijst 7

Deel 1 11

1 Inleiding 13

2 Taken, positie en rol van de FG 15
- 2.1 Introductie 15
- 2.2 Taken 16
- 2.3 Positie 19
- 2.4 Lijnmanagement 21
- 2.5 Profiel van de FG 28
- 2.6 Afronding 31

3 Risicogestuurd werken 33
- 3.1 Introductie 33
- 3.2 Risicosturing 34
- 3.3 Afronding 44

4 Naleving artikel 24 45
- 4.1 Introductie 45
- 4.2 De juiste koers 46
- 4.3 Privacybeleidskader 50
- 4.4 Een passende FG 54
- 4.5 Groeimodel 55
- 4.6 Toetsing aan artikel 24 57
- 4.7 Afronding 58

5 Naleving artikel 25 61
- 5.1 Introductie 61
- 5.2 Een stapje terug 63
- 5.3 Inspelen op artikel 25 66
- 5.4 De functie van DPIA's 68
- 5.5 Gepercipieerd risico 71
- 5.6 Afronding 73

6 Toetsing 75
6.1 Introductie 75
6.2 Incidentele toetsing 76
6.3 Structurele toetsing 82
6.4 Toetsing aan de wet 86
6.5 Doorbraak geheimhouding 87
6.6 Afronding 88

7 Stijl en competenties 91
7.1 Introductie 91
7.2 Stijl 92
7.3 Competenties 96
7.4 Afronding 100

Deel 2 103

Veel gestelde vragen 105
Hoe waardeer je privacyrisico's? 105
Hoe schrijf je een FG-verslag? 108
Hoe beoordeel je een DPIA? 112
Hoe behandel je een klacht? 118
Hoe ziet een FG-statuut eruit? 126
Hoeveel verdient een FG? 128
Hoe goed voldoe je aan het wettelijk FG-profiel? 131

Nawoord 135

Over de auteur 137

Deel 1

1 Inleiding

Hoe ben je FG? Dat is een relevante vraag voor iedereen die FG is, FG wil worden, met FG's te maken heeft of eenvoudig wil weten wat een FG nou eigenlijk doet.

FG staat voor functionaris voor gegevensbescherming of, in het Engels, data protection officer. Op zich is die functie overzichtelijk geregeld in artikel 37-39 van de Algemene Verordening Gegevensbescherming. Dat de theorie zich niet altijd makkelijk laat vertalen naar de praktijk, blijkt uit het feit dat veel FG's het lastig vinden om een goede invulling te geven aan hun rol.

De toelichtingen die aan de eigenlijke wettekst van de AVG voorafgaan – in de vorm van 173 'overwegingen' – bieden weinig houvast. De FG wordt alleen genoemd in overweging 77 en 97.

Het Europees coördinerend orgaan van landelijke toezichthoudende autoriteiten, de European Data Protection Board, stelt in haar FG-richtlijnen weliswaar dat de FG een 'key player' is, maar dit heeft meer betrekking op het 'wat' dan op het 'hoe' van FG-schap. Bij het lezen van de richtlijnen bekruipt je bovendien het gevoel dat de opstellers zelf nooit met hun voeten in de klei hebben gestaan.

De FG-functie is niet nieuw. Zij werd al in 1995 geïntroduceerd in de voorganger van de AVG, EU-gegevensbeschermingsrichtlijn 95/46/EG, en vanaf 1998 in Nederland geregeld via de Wet bescherming persoonsgegevens. Sindsdien zijn er FG's actief en hebben ze gezocht naar manieren om het FG-schap goed te laten werken.

Dit boek verwoordt een aanpak die zich in de praktijk keer op keer heeft bewezen en is geënt op inzichten op het gebied van corporate governance. Centraal in de aanpak staat het creëren van *control* en *accountability* door het verstevigen van de verbinding tussen het dagelijks bestuur van een organisatie en de werkvloer.

Wie een beetje vertrouwd is met corporate governance en de AVG vanaf artikel 24 leest, ziet dat de wetgever eigenlijk niets anders heeft gedaan dan corporate governance wettelijk regelen, maar dan toegespitst op het thema 'bescherming persoonsgegevens'.

Corporate governance klinkt groot, maar de aanpak die je in dit boek aantreft, werkt net zo goed voor kleine ondernemingen, overheidsinstellingen, stichtingen of verenigingen. Vanzelfsprekend is iedere organisatie anders. *Hoe ben je*

FG? reikt je de methodiek aan om oplossingen te vinden die werkelijk passen bij jouw organisatie – want zoals we gaan zien, draait het in de AVG om het woord 'passend'.

Dit boek helpt je om van de FG-functie een succes te maken. Als je het recept van dit boek volgt, beschik je over een werkwijze die duidelijk herkenbaar en begrijpelijk is voor bestuurders, ketenpartners, accountants, riskmanagers, informatiebeveiligers, bedrijfsjuristen, de Autoriteit Persoonsgegevens (AP) en – niet in de laatste plaats – de verschillende doelgroepen waarover je organisatie gegevens verwerkt.

Hoe ben je FG? is een praktische handreiking, geen juridisch handboek. Tegelijkertijd sluit het boek nauw aan bij de eigenlijke tekst van de AVG, de achterliggende bedoelingen ervan en de wetmatigheden van het Europees publiekrecht. Je kunt dit boek ook lezen als een 'richtsnoer' in de betekenis van overweging 77 AVG (dit boek is immers geschreven door een FG).

We beschrijven hoe je als FG op bestuurlijk niveau en operationeel niveau professioneel invulling geeft aan je taken. Aan bod komen je missie, je aanpak en de tools voor het boeken van resultaat, zoals het AVG-kompas, de Schaal van erg, en incidentele en structurele toetsing voor bestuurlijke verslaglegging. Hiermee kun je aan de slag binnen de FG-jaarcyclus. We eindigen met een hoofdstuk over de stijlen en competenties die je nodig hebt om van het FG-schap een succes te maken. In een uitgebreide bijlage geven we antwoord op een aantal veelgestelde vragen. Dit doen we zoveel mogelijk aan de hand van praktijkvoorbeelden.

Over de functie van FG raak je niet snel uitgepraat. Dit boek valt probleemloos uit te breiden met meer hoofdstukken en bijlagen, maar een boek samenstellen is ook keuzes maken. We hebben gekozen voor ingrediënten die samen een doeltreffend antwoord bieden op de vraag 'Hoe ben je FG?'. Hopelijk bieden we daarmee de inspiratie die je zoekt.