FG-as-a-service

ZILVERBLAD informatiebeveiliging

EEN DIENST VAN ZILVERBLAD INFORMATIEBEVEILIGING

De nieuwe Europese privacy wetgeving Algemene Verordening Gegevensbescherming (AVG) verplicht bepaalde organisaties tot het aanstellen van een Data Protection Officer (DPO). Voor Nederland is de formele juridische term Functionaris voor de Gegevensbescherming (FG). De FG houdt binnen de organisatie toezicht op een correcte toepassing van de privacywetgeving.

Voor welke organisaties wordt een FG verplicht?

1. alle overheidsinstanties en -organen;
2. alle bedrijven en organisaties die persoonsgegevens verwerken die *'vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen'*;
3. alle bedrijven en organisaties die op grote schaal persoonsgegevens verwerken *'van bijzondere categorieën van gegevens'* (zoals ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid) en/of persoonsgegevens met betrekking tot *'strafrechtelijke veroordelingen en strafbare feiten'*.

Takenpakket van een FG

De AVG beschrijft welke taken een FG minimaal moet verrichten. De belangrijkste taken van een FG zijn:

- Informeren en adviseren over de wettelijke verplichtingen bij het verwerken van persoonsgegevens en toezien op naleving ervan;
- Toezien op een adequate beveiliging van gegevens en adviseren over betrouwbare ICT (privacy by design);
- Organiseren van een (verplichte) Privacy Impact Assessment (PIA) vóór het starten met nieuwe verwerkingen van persoonsgegevens, waarbij mogelijke risico's voor de privacy van betrokkenen worden geïnventariseerd. NB: voor Nederland is de formele juridische term hiervoor een Gegevensbeschermingseffectbeoordeling (GEB);
- Als aanspreekpunt fungeren voor privacy vragen, zowel intern voor de organisatie zelf als extern voor de betrokkenen waarvan persoonsgegevens verwerkt worden;
- Samenwerken met de Autoriteit Persoonsgegevens (AP).

De wet stelt de volgende eisen aan een FG

- Een FG moet een natuurlijk persoon zijn (mag dus geen commissie, OR of bedrijf zijn);
- Een FG moet voldoende kennis hebben van de organisatie, van informatiebeveiliging en van de privacywetgeving (een CIPP/E-certificering is hiervoor een adequate invulling);
- Een FG moet betrouwbaar zijn, dit uit zich onder meer in een geheimhoudingsplicht.

Bevoegdheden van een FG

Een FG heeft geen formele sanctiebevoegdheden. Maar de organisatie is wel wettelijk verplicht om de FG controle-bevoegdheden te geven. Zo moet een FG bevoegd zijn om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen. De FG moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten binnen een organisatie.

NB: heeft een organisatie een FG, dan behoudt de AP als nationale toezichthouder alle bevoegdheden. De AP stelt zich wel terughoudend op bij organisaties met een FG.

FG-as-a-service

Voordelen van een ingehuurde FG

De wet biedt de mogelijkheid om de verplichting in te vullen met een interne of externe FG. De voordelen van een ingehuurde specialist zijn:

- Kosteneffectiviteit, omdat de functie van FG meestal geen fulltime baan is en extern met een bij de organisatie passende inzet ingehuurd kan worden;
- De benodigde expertise is specialistisch en breed, met een ingehuurde FG (met CIPP/E-certificering) is continuïteit en actualiteit van benodigde kennis gegarandeerd;
- De beschikbare kennis is breder omdat de FG dagelijks bezig is met gegevensbescherming in verschillende werkomgevingen, maar ook kennis opdoet vanuit vakverenigingen (IAPP, ISACA, PvIB);
- De FG heeft als extern persoon geen enkel persoonlijk belang bij politieke gevoeligheden binnen de organisatie en kan daardoor een meer onafhankelijke rol innemen.

Aanstellen van een FG

Een organisatie kan een FG aanstellen d.m.v. een dienstverleningsovereenkomst. De organisatie moet de FG vervolgens aanmelden bij de AP, pas dan kan de FG formeel aan de slag (de FG kan zelf ondersteunen bij de aanmelding). De AP publiceert alle aanmeldingen van FG's in een register, te vinden op de site van de AP.

Inzet is maatwerk

Het 'privacyprofiel' van een organisatie bepaalt in grote mate de benodigde inzet van een FG. Dat 'privacyprofiel' wordt bepaald door omvang en dynamiek van de organisatie, in combinatie met het aantal verwerkingsprocessen van persoonsgegevens en de risico's die daarbij spelen. De benodigde inzet moet daarom altijd per organisatie specifiek ingeschat en afgesproken worden.

Van start

Als de FG van start gaat zal hij beginnen met het aanleggen van een (verplicht) register waar alle verwerkingen van persoonsgegevens van de organisatie in vermeld worden. Vervolgens wordt per verwerking bekeken of deze conform wettelijke eisen is ingevuld en worden eventueel aanbevelingen gedaan voor verbeteringen. Deze opstartfase zal tijdelijk wat meer inzet van de FG vragen. Na de opstartfase valt de inzet terug naar een vaste basis, met daarbij eventueel extra inzet als wijzigingen of omstandigheden daarom vragen.

Het inhuurmodel van Zilverblad

Zilverblad biedt haar 'FG-as-a-service'-dienst aan met een dienstverleningsovereenkomst die gebaseerd is op een combinatie van fixed inzet en fixed bedrag per maand, met daarbij nacalculatie van eventueel extra benodigde inzet boven de verwachte standaard inzet.

Om de toezichthoudende rol van FG in te kunnen vullen zal er altijd minimaal één werkdag per maand aanwezigheid op locatie van de organisatie nodig zijn. Deze dag zit daarom in elk geval in de fixed inzet per maand begrepen. Alle werkzaamheden die niet binnen de basisinzet vallen worden in overleg uitgevoerd en op basis van nacalculatie doorbelast. Eventuele ad hoc vragen of problemen kunnen altijd tussen reguliere afspraken door per mail of telefoon voorgelegd worden aan de FG.

ZILVERBLAD
informatiebeveiliging

Zilverblad Informatiebeveiliging is in 2014 opgericht door Bart van der Kallen (CISM, CIPP/e). Naast de dienst FG is Zilverblad ook ervaren in ISO 27001 / NEN 7510 trajecten en inzetbaar als Information Security Officer. Meer informatie over onze diensten vindt u op onze website www.zilverblad.nl.
CONTACT: Telefoon: 06 13 34 90 83 - Mail: info@zilverblad.nl