INFORMATIE
BEVEILIGINGS
DIENST

Digitaal *be*spreekuur

2 jaar AVG – waar sta je als FG?

IBD

25 mei 2020

VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

Privacyverklaring

De IBD stelt Zoom privacyvriendelijk in (privacy by default)

Tijdens de interactieve webinars maakt de IBD:

- gebruik van wachtwoorden om aan vergaderingen deel te nemen.
- gebruik van unieke vergader ID’s om vergaderingen af te schermen.
- geen gebruik van:
  “cloud recording” en neemt de videoconferentie niet op.
  “local Recording”
  “automatically Transcribe Cloud Recordings”
  “attendee attention tracking”

INFORMATIE BEVEILIGINGS DIENST

Even voorstellen

- Naomi (IBD) moderator
- Privacy adviseurs IBD introduceren thema’s en helpen bij beantwoording vragen

INFORMATIE BEVEILIGINGS DIENST

Doel FG *be*spreekuur

- **Informatieoverdracht en deling → Samen issues bespreken**
- Deelnemers: stellen en beantwoorden vragen
- Contacten onderhouden en nieuwe contacten maken
- Input ophalen voor FAQ en Handreiking FG van de IBD


Happy GDPR Day!
INFORMATIE
BEVEILIGINGS
DIENST
VNG

INFORMATIE
BEVEILIGINGS
DIENST

Welkom ..

AUTORITEIT
PERSOONSGEGEVENS

INFORMATIE BEVEILIGINGS DIENST

Programma *be*spreekuur

1. Inleiding IBD
2. Stellingen voor en door FGs
3. Afgewisseld met vragen voor en door FGs
4. Discussie

INFORMATIE BEVEILIGINGS DIENST

Inleiding

Aanwijzing van FG voor gemeenten sinds 2 jaar verplicht (onder Wbp bestond bevoegdheid).

<u>Regels over invulling taak en positie FG</u>

- AVG art. 37 – art. 39 (positie en taken) + art. 35 AVG (verplicht inwinnen advies DPIA)
- Rechtspraak
- Richtsnoeren FG (WP29, Laatste update 5 april 2017, bekrachtigd door EDPB) & inhoud website Autoriteit Persoonsgegevens
- Uitspraken autoriteiten

INFORMATIE BEVEILIGINGS DIENST

Vraag

Vraag: Hoe wordt de rol als FG nu binnen de gemeente belegt? Hoe ziet de structuur eruit binnen de organisatie? Wie heeft welke verantwoordelijkheden?

INFORMATIE BEVEILIGINGS DIENST

Inleiding

Belangrijk uitgangspunt: Verwerkingsverantwoordelijke of verwerker blijft verantwoordelijk voor naleving van de AVG. FG adviseert en houdt toezicht.

"Over het resultaat van de risicobeoordeling,[..], wordt de functionaris voor gegevensbescherming enkel geïnformeerd, niet geconsulteerd. Dit stemt overeen met artikel 38.1 juncto artikel 39.1. a) AVG die vereist dat de functionaris voor gegevensbescherming adviserend dient op te treden ten aanzien van de verwerkingsverantwoordelijke, maar niet medeverantwoordelijk is voor de eindbeslissing. De Geschillenkamer bevestigt op basis daarvan dat het dat de functionaris voor gegevensbescherming enkel over de eindbeslissing omtrent het risico wordt geïnformeerd." GBA, 28 april 2020.

Kan ik mij als FG zelf aan- of afmelden bij de AP of wijzigingen doorgeven?

Dat kan wel maar het is de taak van uw verwerkingsverantwoordelijke om u als FG aan te melden bij de Autoriteit Persoonsgegevens (AP). En ervoor te zorgen dat deze informatie actueel blijft.

INFORMATIE BEVEILIGINGS DIENST

AVG

Aanwijzing FG (art. 37 AVG)

- Overheidsinstanties en organen wettelijk verplicht (artikel 37 AVG).→ "openbaar lichaam" en "publiekrechtelijke instelling" van de verwerkingsverantwoordelijke of de verwerker.

- Eén FG voor verschillende overheidsinstanties of organen, met inachtneming van hun organisatiestructuur en omvang; de verwerkingsverantwoordelijke of de verwerker moet verzekeren dat één enkele functionaris voor gegevensbescherming, indien nodig bijgestaan door een team, deze taken efficiënt kan uitvoeren ondanks het feit dat hij voor meerdere overheidsinstanties en -organen is aangesteld.

- Voldoende middelen en bereikbaarheid en deskundigheid.

INFORMATIE BEVEILIGINGS DIENST

Aanbevelingen AP

AUTORITEIT PERSOONSGEGEVENS

AP, Aanbevelingen voor een effectieve FG in het ziekenhuis, juni 2019.

INFORMATIE BEVEILIGINGS DIENST

Aanbevelingen AP

Aanbevelingen aan FG's

	Houd een goede balans tussen adviserende en toezichthoudende taken. Probeer meer aandacht te besteden aan de toezichthoudende rol.
	Voorkom dat de adviserende en de toezichthoudende rol met elkaar conflicteren. Maak binnen de organisatie duidelijk welke rol je wanneer inneemt. Regel ook hoe te handelen als er daadwerkelijk sprake is van een belangenconflict.
	Maak duidelijke interne afspraken over de verdeling van verantwoordelijkheden en de rol van de FG, bijvoorbeeld bij een datalek.
	Zoek het contact met de werkvloer en ga het gesprek aan. Wees zichtbaar binnen de organisatie. Zichtbaarheid zorgt ervoor dat medewerkers de FG aanspreken en dat de FG signalen ontvangt over knelpunten in de naleving van de AVG.
	Leer van elkaar. Zoek contact en wissel ervaring en kennis uit met andere FG's in de regio of bij andere zorgaanbieders in het land. Veel FG's hebben te maken met dezelfde problematiek. Onderling contact voorkomt dat ze het wiel opnieuw moeten uitvinden.

AUTORITEIT PERSOONSGEGEVENS

INFORMATIE BEVEILIGINGS DIENST

Onderwerpen vandaag

Positie FG (art. 38 AVG)

FG & verwerkingsverantwoordelijke:

- Tijdig betrokken worden [niet alleen informeren maar ook consulteren!]
- Toegang tot persoonsgegevens en verwerkingsactiviteiten en ter beschikkingstelling van middelen.
- Geen instructies met betrekking tot de uitvoering van zijn taken (geen ontslag of straffen voor de uitvoering van zijn taken).
- Rechtstreeks verslag uit aan de hoogste leidinggevende.

FG & betrokkenen: Betrokkenen kunnen te allen tijde contact opnemen met FG.

FG & AP: FG = contactpunt.

INFORMATIE BEVEILIGINGS DIENST

GBA oordeel

Belgische AP legt boete op van EUR 50.000 aan Proximus (GBA, 28 april 2020)

- **Onvoldoende betrokkenheid FG bij melding datalekken niet vastgesteld (art. 38 lid 1 AVG)**
  - De functionaris voor gegevensbescherming van de verweerder behoeft enkel geïnformeerd te worden over het resultaat van de risicobeoordeling (consultatie is nodig bij risicobeoordelingsproces). De FG dient adviserend op te treden ten aanzien van de verwerkingsverantwoordelijke, maar is niet medeverantwoordelijk voor de eindbeslissing.

- **Belangenconflict wel vastgesteld (art. 38 lid 6 AVG)**
  - De FG vervulde naast FG functie ook de functie van directeur audit, risk en compliance.

INFORMATIE BEVEILIGINGS DIENST

Uitgangspunten belangenverstrengeling

- De FG kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden. (Art. 38 lid 6 AVG)
- De FG mag geen functie bekleden waarbij hij de doelstellingen van en de middelen voor de verwerking van persoonsgegevens moet bepalen.
- Conflicterende functies:
  - Hogere management functies (bv. Chief Executive, Chief Operating, Chief Financial, Chief Medical Officer, hoofd van de marketingafdeling, hoofd van Human Resources of hoofd van de IT-afdeling), maar ook lagere functies binnen de organisatiestructuur als deze personen de doelstellingen van en middelen voor de verwerking van gegevens moeten bepalen (EDPB (WP29, FG Richtsnoeren)).
  - CISO

INFORMATIE BEVEILIGINGS DIENST

GBA oordeel

Belangenconflict

1. Conflicterende taken: Niet beperkt tot de gevallen waar een persoon het doel en de middelen van de verwerking bepaalt.

“Het bestaan van een belangenconflict is echter niet beperkt tot de gevallen waar een persoon het doel en de middelen van de verwerking bepaalt. Belangenconflicten moeten steeds geval per geval worden beoordeeld. Het voormelde schrijven van de verweerder toont aan dat haar functionaris voor gegevensbescherming meer doet dan de verweerder intern te adviseren aangezien die persoon binnen [Proximus] conflicterende taken uitvoert die een ***aanzienlijke operationele verantwoordelijkheid inhouden voor gegevensverwerkingsprocessen die vallen onder het domein audit, risk en compliance***.”

INFORMATIE BEVEILIGINGS DIENST

GBA oordeel

Belangenconflict

2. Rechtsleer Duitsland: die […] verwijzen naar criteria zoals (1) het al dan niet bestaan van zelfcontrole door een toonaangevende functiehouder binnen de onderneming, (2) het al dan niet bestaan van interne regels voor belangenconflicten, en (3) het dragen van een belangrijke operationele verantwoordelijkheid met een impact op persoonsgegevens.

3. Afwezigheid beleid over onafhankelijke werkwijze FG

INFORMATIE BEVEILIGINGS DIENST

Vraag over de pettenproblematiek

FG adviseert en houdt toezicht terwijl taken niet mogen conflicteren.

- **Vraag**: Hoe kunnen deze taken van elkaar worden gescheiden?

INFORMATIE BEVEILIGINGS DIENST

Stelling

- **Casus**: Ook al ben ik FG, door het ontbreken van een effectieve privacy organisatie, voer ik voornamelijk Privacy Officer taken uit.

- **Stelling**: De beste oplossing is om te stoppen met het uitvoeren van de operationele privacy taken, met alle gevolgen van dien. Dat is beter dan beide rollen (FG en PO) uitvoeren waarbij beide rollen niet goed uit de verf komen.

V EENS **ONEENS**

INFORMATIE BEVEILIGINGS DIENST

Stelling

- **Stelling**: De FG maakt de inventaris voor het verwerkingsregister.

INFORMATIE BEVEILIGINGS DIENST

Stelling

- **Stelling**: Het is geen probleem als de FG in de hiërarchische lijn bv JZ wordt geplaatst.

INFORMATIE BEVEILIGINGS DIENST

Stelling over de FG en toezicht

- **Stelling**: Het afnemen van interne audits is een effectieve manier om intern toezicht te houden.

INFORMATIE BEVEILIGINGS DIENST

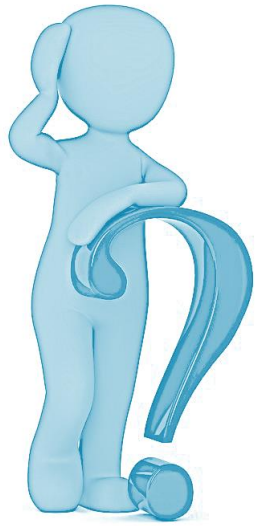
Vraag

- **Vraag**: Hoe borg je de vroegtijdige betrokkenheid van de FG in een gemeentelijke organisatie (Privacy by Design)?

INFORMATIE BEVEILIGINGS DIENST

Vraag

- **Vraag**: Hoe overtuig je directie en management dat zij verantwoordelijk zijn voor privacy?

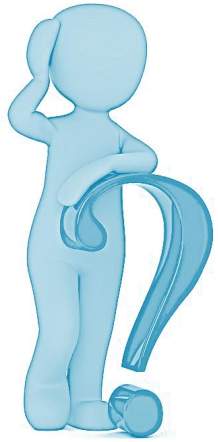


INFORMATIE BEVEILIGINGS DIENST

Vraag

FG adviseert en houdt toezicht terwijl taken niet mogen conflicteren. FG geeft advies en aanbevelingen aan de verwerkingsverantwoordelijke (bestuurder).

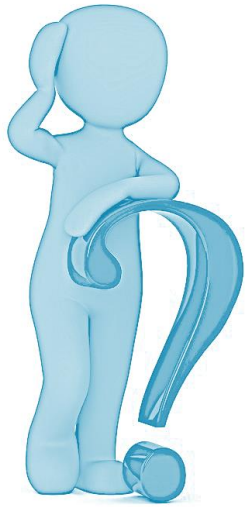
Vraag: Wat kun je als FG als de bestuurder de aanbevelingen van de FG niet opvolgt?

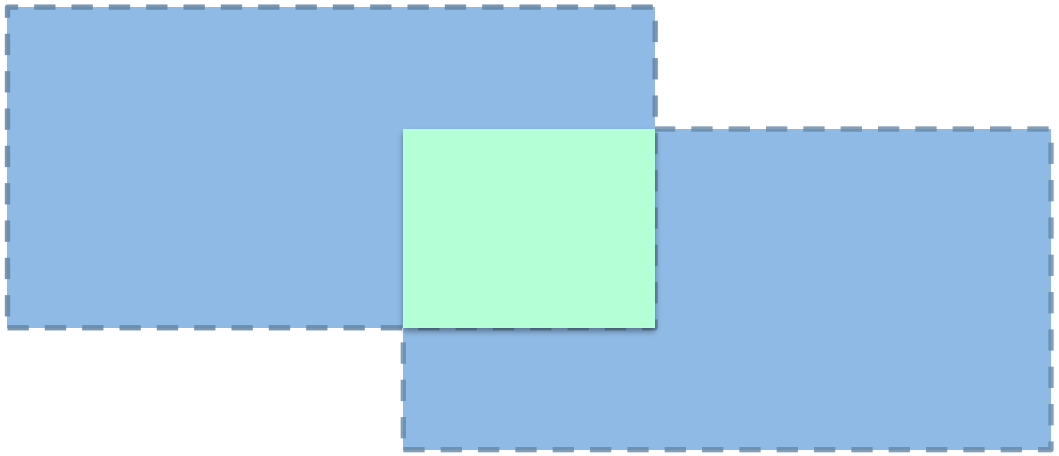


INFORMATIE BEVEILIGINGS DIENST

Vraag

Vraag: Er bestaat nog wel eens onduidelijkheid over de rol van de FG bij samenwerkingsverbanden wanneer sprake is van gemeenschappelijke verantwoordelijkheid. Hoe zit dat precies?





INFORMATIE BEVEILIGINGS DIENST

Vraag over de pettenproblematiek

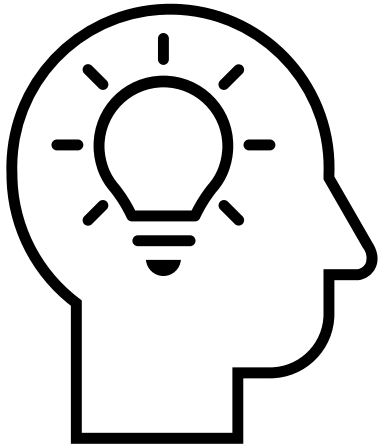
FG adviseert en houdt toezicht terwijl taken niet mogen conflicteren.

- **Vraag**: De onafhankelijke rol van de FG binnen de organisatie: In hoeverre mag een FG bijvoorbeeld ook training, advies en toelichting geven, naast de toezichthoudende rol?

INFORMATIE BEVEILIGINGS DIENST

Vraag FG & betrokkenen

Vraag: Hoe zien awarenessprogramma's eruit voor de algemene werkgevers en de nieuwe medewerkers? Wat werkt wel wat werkt niet.



INFORMATIE BEVEILIGINGS DIENST

Vraag FG & de AP

- **Vragen**: De steun van de AP die we zouden kunnen gebruiken. Hoe zit het met de adviesrol van de AP richting FG's. De ervaring van FG's (van mijzelf en van collega's in de regio of o.b.v. berichten op VNG forum Privacy) is dat de antwoorden vaak weinig concreet of richtinggevend zijn. Waarom kan de AP niet met concretere en richtinggevende antwoorden te komen waar de FG’s nog meer aan hebben? Kan er mogelijk een aparte adviesorganisatie binnen de AP of zo nodig daarbuiten opgezet waardoor een eventueel pettenprobleem zich niet meer voordoet?

INFORMATIE BEVEILIGINGS DIENST

Resterende vragen

Resterende vragen / opmerkingen:

- DPIA proces:
  - Hoe pakken collega's het proces rondom DPIA’s op, rekening houdend met ieders taken en verantwoordelijkheden hierin en met welke diepgang voeren zij deze DPIA's uit. Zijn er uitgewerkte voorbeelden?
  - Gaan we naast een DPIA in veel gevallen ook een DEDA adviseren?
- Compliance:
  - Gedragscode voor alle gemeenten een kans of een utopie? rol VNG hierin?
  - Goede bedoelingen. Soms willen we als gemeente iets wat echt de burger kan helpen. Maar wat niet altijd mag vanuit de AVG. Hoe kun je daar het beste mee omgaan?
  - Hoe voorkomen we dat registreren voor het registreren?

INFORMATIE BEVEILIGINGS DIENST

Handreiking IBD/VNG

Handreiking positionering Functionaris Gegevensbescherming (FG) & Handreiking rol en taken van de Functionaris Gegevensbescherming (FG) zijn samengevoegd.

Met input van vandaag wordt het product gefinaliseerd en gepubliceerd

INFORMATIE BEVEILIGINGS DIENST

Evaluatie bespreekuur

Adviezen en tips voor verbetering?

Suggesties voor vervolgonderwerpen?

- **Niet behandelde vragen worden besproken in een volgend (be)spreekuur – datum volgt**

- Contact: privacy@vng.nl

INFORMATIE BEVEILIGINGS DIENST

Vervolg

- Woensdag 27 mei as om 10:30: Thema Big Data & Open Data

of

- Woensdag 10 juni om 13:00 tot 14:30: Thema Big Data & Open Data

- Contact: privacy@vng.nl