## 13 situaties waarin de functioneel beheerder en de privacyprofessional elkaar aanvullen

# PRIVACYRISICO'S IN KAART BRENGEN?

# PRAAT MET DE FB'ER

De invoering van de AVG heeft impact op de informatievoorziening van bijna elke organisatie. Uiteraard raakt dit het vakgebied privacy, maar ook functioneel beheer. Beide vakgebieden zijn zich er misschien nog niet van bewust, maar ze hebben elkaar nodig. Bij een goede samenwerking kunnen ze elkaar zelfs versterken. Daniël Brouwer en Jeroen Wittink raden de functioneel beheerder en de privacyprofessional dan ook dringend aan elkaar op te zoeken.

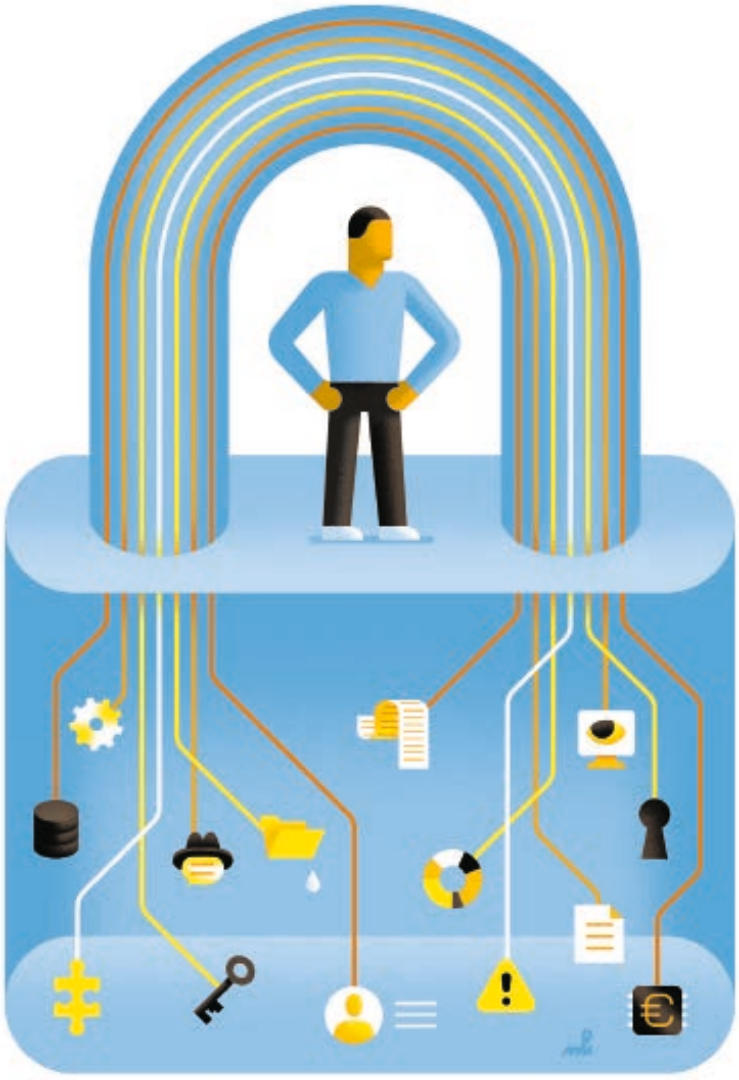
door Daniël Brouwer en Jeroen Wittink illustratie Marc Kolle

DE UITKOMST VAN DE VOLGENDE DERTIEN SITUATIES IS OPTIMAAL WANNEER DE FUNCTIONEEL BEHEERDER EN DE PRIVACYPROFESSIONAL ELKAAR OPZOEKEN, WETENDE WAT ZE VAN ELKAAR KUNNEN EN MOGEN VERWACHTEN.

De functioneel beheerder is de spin in het informatieweb van een organisatie. De primaire taak van een functioneel beheerder is te zorgen voor een betrouwbare, wendbare, schaalbare en innovatieve informatievoorziening. Hij/zij ziet veel, hoort veel en heeft veel impliciete kennis over processen, applicaties, leveranciers en het gebruik van ICT binnen de organisatie. De functioneel beheerder is ook bekend met de schaduwkant van de IT-organisatie, een belangrijke bron van risico's. Dit maakt de functioneel beheerder van onschatbare waarde voor de privacyprofessional.

### 1. HOE STROMEN DE PERSOONSGEGEVENS?

Voor een gedegen privacybeleid is het van fundamenteel belang om de informatiestromen in kaart te brengen. Op basis van de informatie-inventarisatie neemt de privacyprofessional



**"STREEF NAAR EXPLICIETE KENNIS OP SCHRIFT"**

beslissingen en maatregelen om te voldoen aan de AVG en andere wetgeving. Een correcte en nauwkeurige registratie is daarom van belang voor de privacyprofessional.
Binnen organisaties zijn er beheerde en onbeheerde informatiestromen. Een functioneel beheerder kan helpen om beide stromen in kaart te brengen. Met name de onbeheerde stromen vormen een belangrijk privacyrisico. Deze stromen zijn niet beschreven en liggen slechts vast in de hoofden van de medewerkers en zijn bij uitval van ldeze medewerkers niet geborgd in de organisatie.

## 2. REGISTER VAN VERWERKINGEN

Onder de AVG is het bijhouden van een 'register van verwerkingen' verplicht. Dit register is de informatieboekhouding van de organisatie. Het vormt de basis van het beleid om te voldoen aan de AVG. Welke gegevens heeft de organisatie? Op basis van welke grondslag zijn deze verzameld? Wat mag de organisatie doen met deze informatie?
Vaak wordt de proces- en applicatie-eigenaar betrokken bij het opstellen van het register. De functioneel beheerder kan een belangrijke controleslag uitvoeren voor de registers, omdat hij/zij inzicht heeft in de daadwerkelijke – beheerde en onbeheerde –informatiestromen.
Ook kan de functioneel beheerder verwerkersovereenkomsten controleren, met name de overeenkomsten die door leveranciers zijn aangeleverd. Ook kan het register van verwerkingen normstellend werken: het geeft de toegestane verwerkingen binnen een proces, informatieketen of applicatie weer.

## 3. EXPLICIETE EN IMPLICIETE KENNIS

Het opstellen en beheren van de applicatiedocumentatie en applicatieprocessen ligt vaak op het bord van de functioneel beheerder. Kwalitatief goede documentatie maakt medewerkers risicobewust en demonstreert wat wel en wat zeker niet is toegestaan in de applicatie. Het register van

"De ervaring leert dat circa 30% van de applicaties niet wordt beheerd"

## WAT DE FUNCTIONEEL BEHEERDER NIET KAN

De functioneel beheerder is vaak een schaap met vijf poten, maar hierin schuilt ook een risico. Veel taken vallen buiten de officiële functiebeschrijving van de functioneel beheerder, terwijl deze functie hiervoor wel wordt ingezet: beslissingen nemen, het voeren van projectmanagement en de rol van auditor c.q. controleur. Uiteindelijk hoort functioneel beheer een operationele functie te zijn binnen de organisatie. Het ruimer inzetten van functioneel beheer is opnieuw risicovol.

verwerkingen werkt normatief. Het wordt echt spannend als de applicatiekennis vooral tussen de oren van een functioneel beheerder is opgeslagen. Impliciete kennis is natuurlijk ook kennis, echter het Brein Informatie Centrum (BIM) is niet geschikt om alle informatie voor altijd op te slaan. Wordt de impliciete kennis in meerdere BIM's opgeslagen, dan is het spanningsveld compleet. Streef naar expliciete kennis op schrift.

### 4. MAATWERK EN PLEISTER-SOFTWARE

Als een applicatie 'maatwerk' bevat en dus afwijkt van de standaardwerken, brengt dit een (privacy)risico met zich mee. Bijvoorbeeld bij het maken van updates, het implementeren van changes en het aangaan van overeenkomsten met leveranciers. Slecht beschreven maatwerk is ook impliciete kennis en wordt gezien als een aanzienlijk privacyrisico.

### 5. WANDELGANGEN INFORMATIE SYSTEEM (WIS)

De functioneel beheerder kent vaak het gehele speelveld rond een applicatie, proces of organisatieonderdeel. Hij/zij praat met iedereen en weet daardoor veel. Functioneel beheer is een laagdrempelige functie, waardoor medewerkers zich eerder hier zullen melden dan bij de privacyprofessional. De functioneel beheerder is bekend met de sentimenten van de gebruiker, kent het gebruik én de business.

### 6. OPERATIONELE RISICO'S

Informatieveiligheid is risicomanagement op het gebied van informatie. De functioneel beheerder weet vaak hoe applicaties en IT in de praktijk worden gebruikt. Zo nemen secretariaten geregeld hr-zaken uit handen van managers en worden gegevens uit de applicatie handmatig aangepast of overgetypt in een ander systeem.
De functioneel beheerder kent veelal de zwakheden van een systeem. Hoe kan dit systeem gehackt worden? Welke risico's zie jij in de praktijk? De antwoorden van de functioneel beheerder op deze vragen geven gegarandeerd stof tot nadenken.

### 7. OVERZICHT VAN INCIDENTEN, VERZOEKEN

Veel organisaties beschikken niet over een – volledig – overzicht van privacygerelateerde incidenten. De functioneel beheerder heeft echter vaak wel weet van incidenten, van zaken die onder de radar zijn gebleven of niet zijn geëscaleerd. De functioneel beheerder weet of er verzoeken zijn gedaan in het kader van de AVG, zoals inzage van verzamelde persoonsgegevens, rectificatie en recht op vergetelheid. Mogelijk zijn er meldenswaardige incidenten geweest die in de lijn zijn opgepakt, maar niet als zodanig zijn geregistreerd in het overzicht van incidenten.

### 8. ADIDAS-KOPPELINGEN

De uitwisseling van persoonsgegevens tussen applicaties is een aandachtspunt in elke DPIA (data protection impact assessment).
Tijdens een DPIA wordt bijvoorbeeld gekeken naar de privacyrisico's binnen een applicatie.
Persoonsgegevens zijn op basis van een expliciet doel en een grondslag verzameld. Doel en grondslag moeten gedurende de gehele levenscyclus van de data gewaarborgd blijven. Met name Adidas-koppelingen vormen een risico: dit zijn koppelingen die manuele handelingen bevatten of afhankelijk zijn van menselijk handelen. De data gaan dus niet alleen over de 'lijn', maar worden ook gezien door een mens, met alle risico's van dien.
De functioneel beheerder weet hoe applicaties met elkaar zijn verbonden en kent ook de onofficiële connecties, geitenpaadjes en datastromen die nog handmatig worden aangepast.

## MAAK SNEL EEN AFSPRAAK MET ELKAAR

De kracht van een functioneel beheerder is dat hij/zij diep in de organisatie zit en weet wie wat doet, wie de diverse belanghebbenden zijn, hoe de processen lopen maar vooral ook hoe er om processen heen wordt gelopen. De functioneel beheerder kent de risico's, zwakheden en kansen van een proces en applicatie. Daarom is de functioneel beheerder zo'n belangrijke partner voor de privacyprofessional.

### 9. ONEIGENLIJK GEBRUIK

Het grootste privacyrisico vormt het oneigenlijk gebruik van applicaties en systemen: het gebruik van een applicatie of systeem buiten de vastgelegde afspraken en processen om. Er is sprake van oneigenlijk gebruik als bijvoorbeeld het bsn wordt ingevuld in een memoveld, data worden gecombineerd zonder wettelijke grondslag en dit gebruik niet langer het eerder vastgestelde doel dient. Een functioneel beheerder kent het daadwerkelijke gebruik van de applicatie en kan de privacyprofessional wijzen op risico's en oneigenlijk gebruik.

### 10. SCHADUW-IT

Schaduw-IT is een belangrijk privacyrisico, omdat het moeilijk te beheersen is en meestal niet in kaart is gebracht. De ervaring leert dat circa 30% van de applicaties niet wordt beheerd. Deze applicaties zijn niet officieel goedgekeurd, maar worden wel vaak gebruikt om persoonsgevoelige data uit te wisselen. WhatsApp wordt bijvoorbeeld vaak gebruikt om bijzondere persoonsgegevens uit te wisselen. Deze schaduw-IT ontstaat doordat business en IT niet goed op elkaar aansluiten.

De functioneel beheerder kent de schaduwkant van de IT-organisatie en kan helpen nieuwe applicaties in te richten en bestaande applicaties te verbeteren.

### 11. IMPLEMENTEREN VAN OPLOSSINGEN

Elk DPIA of een ander type audit leidt tot aanbevelingen, verbeterpunten en maatregelen die geïmplementeerd moeten worden. De functioneel beheerder signaleert situaties waarin business en IT niet goed op elkaar aansluiten en kan de privacyprofessional adviseren over de implementatie van maatregelen op operationeel niveau. Wordt het gewenste doel bereikt? Is het een realistische maatregel, of gaan gebruikers de maatregel omzeilen?

### 12. ROL BIJ INCIDENTEN EN DATALEKKEN

Tijdens een incident moet de organisatie onder druk beslissen. Het is belangrijk dat de juiste informatie voorhanden is, bijvoorbeeld over het aantal datasubjecten dat betrokken is bij een datalek en welke informatie toegankelijk is geweest. De functioneel beheerder toont zijn/haar toegevoegde waarde als hij/zij de crisismanager op het juiste moment voedt met de meest accurate informatie. Daarnaast is de functioneel beheerder in staat voorlichting te geven aan eindgebruikers.

### 13. AUTORISATIEBEHEER EN TOEGANGSBELEID

Elke ongeautoriseerde toegang tot informatie is een datalek. Dit kan ook ongeautoriseerde toegang zijn door een medewerker binnen de organisatie tot bijvoorbeeld patiëntendossiers.
De functioneel beheerder is bekend met de toegangsrechten binnen een applicatie. Vaak heeft de functioneel beheerder deze autorisatiematrix zelf ingeregeld en geoperationaliseerd, op basis van de behoefte van de organisatie.

## REACTIES EN BIJDRAGEN

Voor reacties en nieuwe bijdragen van IT-experts:
Tanja de Vrede
020-2356415
t.d.vrede@agconnect.nl

## AUTEURS

DANIËL BROUWER is Lean Six Sigma Master Black Belt en expert op het gebied van functioneel beheer. Hij is interimmanager, ondernemer en spreker en daarnaast auteur van 'Hét handboek voor de functioneel beheerder' en oprichter van de vakopleiding functioneel beheer.

JEROEN WITTINK is managing partner bij Factor50 Informatieveiligheid. Zijn aandachtsgebied is risicomanagement en informatieveiligheid. Jeroen is voornamelijk werkzaam binnen de zorg, het onderwijs en het notariaat.