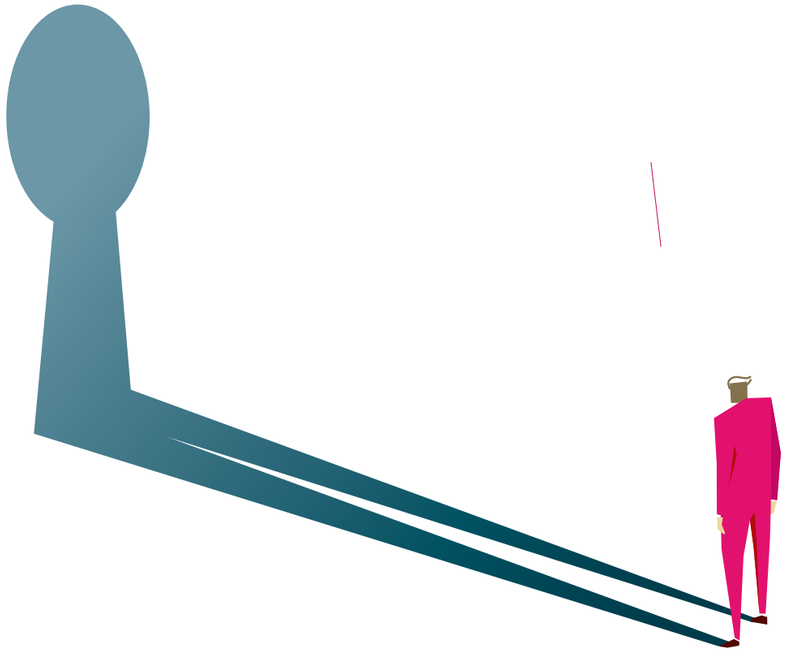
Nationale Privacy Benchmark 2017

VERDONCK KLOOSTER & ASSOCIATES

ECP

Platform voor de InformatieSamenleving

Inhoud



Inleiding

We staan op de drempel van een belangrijk jaar. Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De benodigde aanpassingen zijn ingrijpend. Zo is het belangrijker geworden om aan te tonen hoe de wet nageleefd wordt. Ook heeft de toezichthouder een grotere boetebevoegdheid gekregen.

VKA heeft voor het derde jaar een enquête onder Nederlandse organisaties uitgevoerd naar privacybescherming en AVG-gereedheid. Dit jaar is het onderzoek gedaan in samenwerking met ECP - als neutrale aanjager van een betrouwbare digitale samenleving. Waar staat Nederland, een half jaar voor uur U?

Er zijn interessante inzichten te destilleren. Er is in 2017 duidelijk werk gemaakt van privacybescherming. Zo hebben bijna 90 van de 100 ondervraagden protocollen voor PIA's en datalekken. Toch durft een kwart niet volmondig 'ja' te antwoorden op de gewetensvraag of men als klánt vertrouwen zou hebben in de omgang met persoonsgegevens. In dit rapport kunt u lezen welke zaken volgens de geënquêteerden beter kunnen.

We hopen dat de Nationale Privacy Benchmark 2017 inzichtelijk maakt hoe uw organisatie zich vergelijkt met het nationale beeld en dat het aandacht genereert voor die zaken, die nog extra aandacht behoeven in de periode tot 25 mei. We wensen u succes in het AVG-gereed maken van uw organisatie!

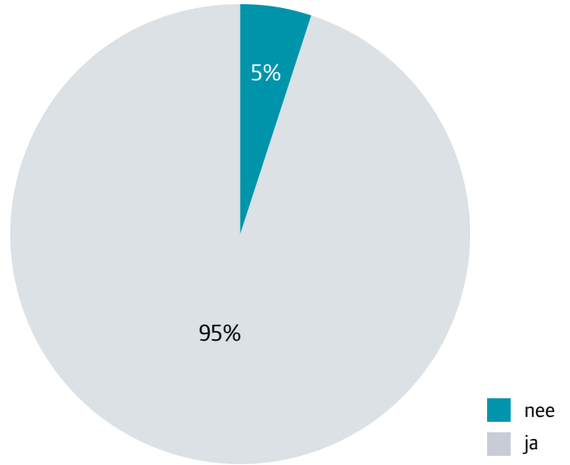
Frank van Vonderen
Partner Verdonck, Klooster en Associates

Arie van Bellen
Directeur ECP | Platform voor de InformatieSamenleving

Hoe is privacy verankerd binnen organisaties?

Vraag:

Heeft de verantwoorde omgang met persoonsgegevens de komende drie jaar een expliciete prioriteit voor uw organisatie?



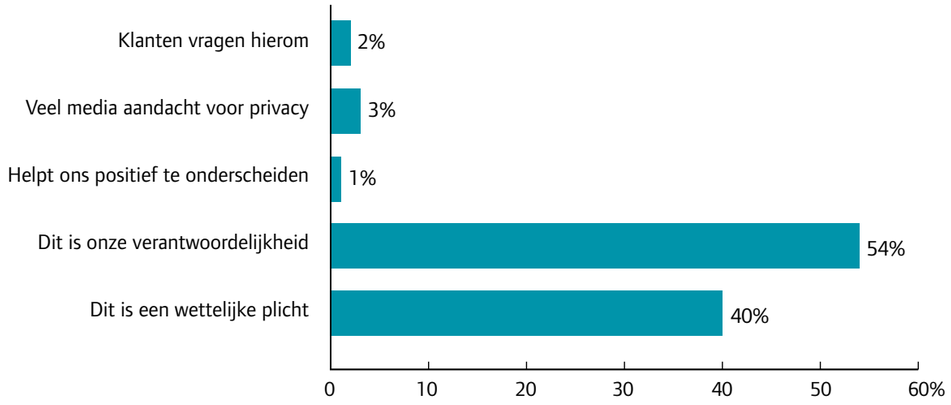
Het is overduidelijk dat de respondenten van mening zijn dat de bescherming van persoonsgegevens de komende jaren een expliciete prioriteit zal zijn voor organisaties.

De resultaten van dit jaar zijn vergelijkbaar met de resultaten van de Nationale Privacy Benchmark (NPB) in 2015 en 2016. Ook toen vond meer dan 90% van de deelnemers dat de bescherming van persoonsgegevens de komende jaren een expliciete prioriteit zal zijn.

Hiermee ligt er een goede basis voor organisaties om de komende jaren de nodige aandacht te besteden aan de bescherming van persoonsgegevens.

Vraag:

Wat is de belangrijkste aanleiding om persoonsgegevens te beschermen?



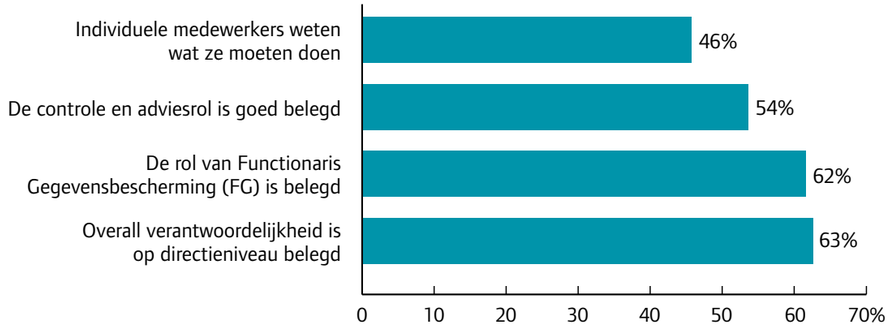
Het beschermen van persoonsgegevens blijkt vooral een hygiëne factor te zijn. Iets wat je organisatie doet, gewoon omdat je een verantwoordelijkheid hebt of aan een wettelijke plicht moet voldoen.

Andere aanleidingen die uitgaan van een meer intrinsieke belangstelling voor privacy, zoals ‘vraag van klanten’ en ‘helpt positief profileren’ blijken geen driver voor Privacy. Deze antwoorden zijn in nog geen 10% van de gevallen de aanleiding.

Vraag:

Welke verantwoordelijkheden voor privacy zijn binnen uw organisatie goed belegd?

(meerdere antwoorden mogelijk)



Privacy is binnen een organisatie niet alleen een zaak voor een privacy officer, maar is de verantwoordelijkheid van iedere werknemer. Dit houdt bijvoorbeeld in dat:

- de directie eindverantwoordelijk is;
- de lijnmanagers gedelegeerd verantwoordelijk zijn;
- de medewerkers zich houden aan de geldende afspraken;
- is voorzien in een controle en adviesrol.

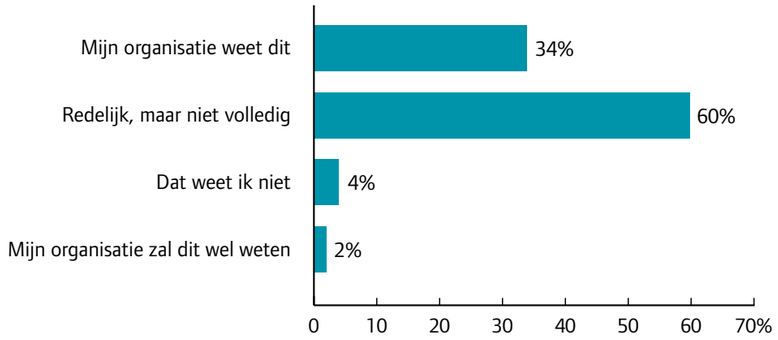
Het goed beleggen van de rollen en verantwoordelijkheden is een belangrijke randvoorwaarde om als organisatie effectief de benodigde acties te kunnen beleggen. De benchmark laat zien dat deze taken en rollen ten dele zijn belegd, maar dat er ook nog wel het nodige is te doen.

Ten opzichte van 2015 en 2016 zijn de verantwoordelijkheden beter belegd bij de directie en bij de Functionaris Gegevensbescherming (FG). Deze rollen zijn bij bijna tweederde van de organisaties belegd, wat een duidelijke stap voorwaarts is ten opzichte van de NPB 2016. Toen was de rol van de FG bij 35% van de organisatie belegd en de overall verantwoordelijkheid bij 44%.

Bij een meerderheid van de deelnemers (54%) is het uitleggen van de verantwoordelijkheden aan medewerkers nog een aandachtspunt. In de praktijk is zichtbaar dat dergelijke awareness activiteiten (waarin aan medewerkers wordt uitgelegd wat van hun wordt verwacht) aan het einde van een verbetertraject zijn gepland.

Vraag:

In hoeverre weet u waar de persoonsgegevens binnen uw organisatie worden gebruikt?



De basis voor een goede bescherming van persoonsgegevens is dat je als organisatie ook weet waar zich binnen een organisatie persoonsgegevens bevinden.

In 2016 had tweederde hiervan geen goed beeld. In 2017 is op dit punt een verbetering zichtbaar al constateert meer dan de helft (60%) dat het beeld nog niet volledig is.

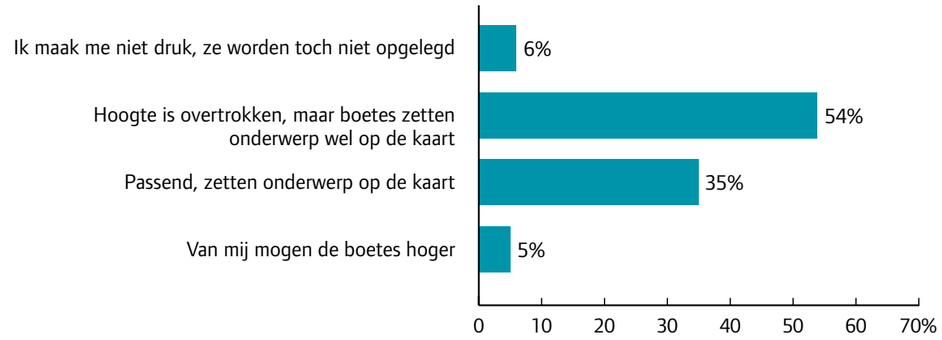
In onze ervaring concentreren persoonsgegevens zich in specifieke systemen (HR, clientsystemen, et cetera). Daarnaast komen persoonsgegevens voor in generiek ondersteunende voorzieningen als mail, office of in document management systemen. Het traceren van persoonsgegevens in dergelijke ondersteunende systemen is een enorme uitdaging omdat dit vaak ongestructureerde gegevensverzamelingen zijn. Dit resulteert in specifieke risico's bij de bescherming van data en bij de verplichting deze te verwijderen. Ook verhindert deze ongestructureerde gegevens-verzameling de uitoefening van rechten van betrokkenen (zoals rechten op inzage, correctie en verwijdering). Immers: als niet duidelijk is in welke ongestructureerde data welke persoonsgegevens zijn opgenomen kunnen deze rechten niet effectief worden uitgeoefend.

Ook de incidentele verzamelingen (éénmalig klantenonderzoek, de medewerkerslijst voor de kerstpakketten, de sollicitatiebrieven, et cetera) bevinden zich regelmatig buiten het blikveld van de organisatie.

Vraag:

Wat vindt u van de boetebedragen voor privacy schendingen?

(meerdere antwoorden mogelijk)

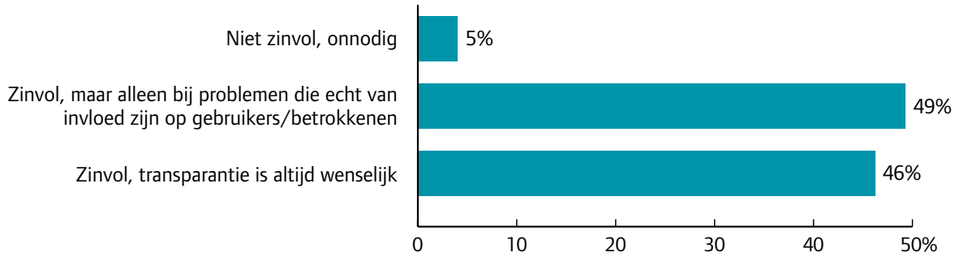


De boetes die kunnen gelden bij een schending van de privacy wetgeving is voer voor menige discussie. Overwegend zijn de deelnemers van mening dat de boetes qua hoogte overtrokken zijn, maar dat zij wel helpen om het onderwerp op de kaart te zetten.

Saillant detail is dat alleen vanuit de publieke sector is gekozen voor de meest extreme antwoordcategorieën: 'Ik maak me niet druk, ze worden toch niet opgelegd' en 'Van mij mogen de boetes hoger'.

Vraag:

De meldplicht datalekken is achteraf gezien...



De Wet Meldplicht Datalekken verplicht organisaties om datalekken te melden. Doet men dat niet, dan kan dit leiden tot sancties.

De meldingsplicht gaat uit van twee soorten meldingen. Allereerst aan de toezichthouder, de Autoriteit Persoonsgegevens (AP) en ten tweede aan de betrokkene, de persoon wiens gegevens zijn gelekt.

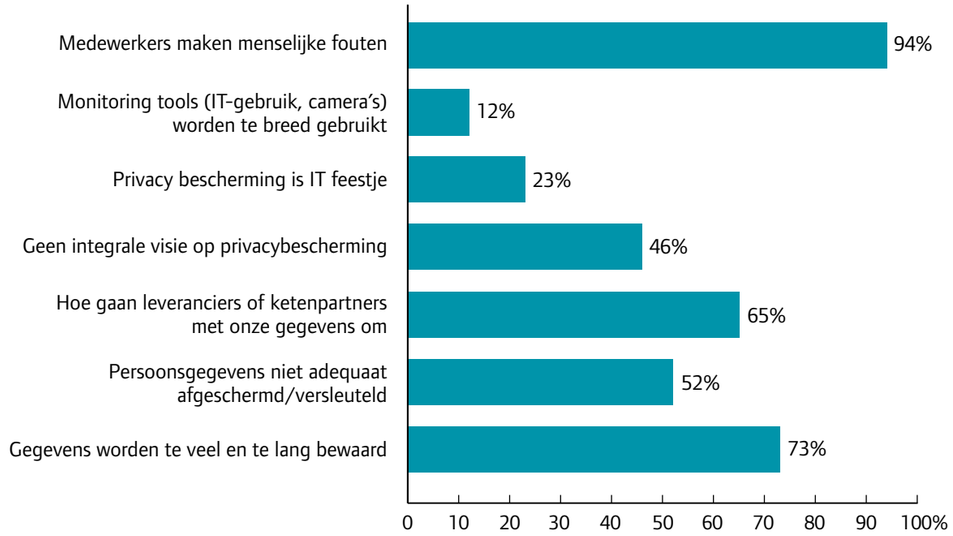
Aan de AP wordt bijvoorbeeld gemeld wat er is gebeurd en wat er is gedaan om het lek te verhelpen. De melding aan de betrokkene hoeft alleen als het waarschijnlijk is dat het lek tot een risico kan leiden voor de betrokkene.

Over de zin van de meldplicht zijn de respondenten het vrijwel anoniem eens. De kanttekening hierbij is dat de helft van mening is dat de meldplicht vooral zinvol is als er problemen zijn die werkelijk van invloed zijn op de persoonlijke levenssfeer van de betrokkenen.

In de praktijk zien wij een groeiende weerstand tegen wat het 'melden om het melden' wordt genoemd: hiervan is bij voorbeeld sprake als er in theorie sprake is van een datalek, maar op geen enkele manier hard kan worden gemaakt dat feitelijk gegevens zijn gelekt of dat betrokkenen hier last van ondervinden. In dat geval geldt wel de meldplicht bij de AP.

Vraag:

Welke aspecten vormen een belangrijk risico op het vlak van privacybescherming?



Deze resultaten lijken definitief de mythe te ontkrachten dat technische maatregelen afdoende zijn om persoonsgegevens te beschermen. Volgens de respondenten zijn de organisatorische risico's en consequenties van het onzorgvuldig menselijk handelen de belangrijkste risico's voor privacy bescherming.

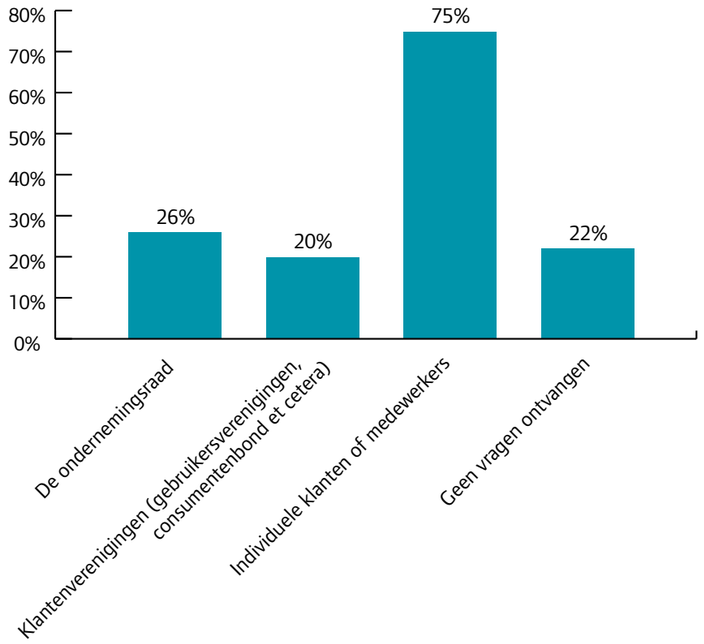
Meer dan 90% ziet het onzorgvuldig menselijk handelen ook als het belangrijkste risico.

Daarnaast scoort het organisatorische risico 'gegevens worden te veel en te lang bewaard' opnieuw hoog met 73%, net als in 2015 en 2016. De neiging om te veel en te lang te bewaren is hardnekkig en in strijd is met andere ontwikkelingen, waarbij veel data wordt verzameld om deze ook later te kunnen correleren. Deze uitdaging zal blijven groeien: bij digitalisering is vaak niet nagedacht over bewaartermijnen en over hoe gegevens (selectief) kunnen worden verwijderd. Dit zou geïncorporeerd moeten worden in 'Privacy by Design'.

Ook de afhankelijkheid van leveranciers en ketenpartners is een erkend risico voor tweederde van de deelnemers. De privacywetgeving vraagt niet alleen dat verantwoordelijke, verwerker en subverwerker helder naar elkaar zijn over de verwachtingen en afhankelijkheden op het punt van adequate bescherming van persoonsgegevens. Ook vereist de wet dat men onderling toeziet op de feitelijke uitvoering van afspraken.

Vraag:

Van welke partijen heeft u de afgelopen periode vragen gehad over de bescherming van persoonsgegevens? (meerdere antwoorden mogelijk)



Een van de belangrijke onderdelen van de privacywetgeving is dat organisaties transparant moeten zijn over de persoonsgegevens die men verwerkt.

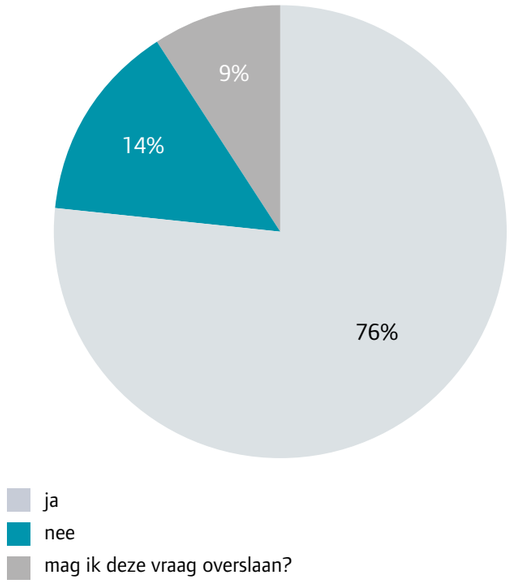
Onderdeel daarvan is ook dat een organisatie zich verantwoordt en antwoord geeft op vragen die worden gesteld. Maar wie stelt deze vragen?

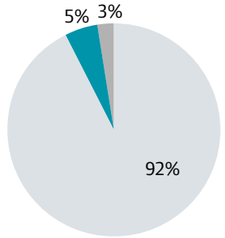
De vragen die organisaties krijgen zijn vooral afkomstig van individuele klanten en medewerkers.

Een goede communicatie over de omgang met de persoonsgegevens wordt daarmee steeds belangrijker. Steeds meer zien wij dat organisaties niet alleen een formeel privacyreglement hanteren, maar ook een makkelijker leesbare variant publiceren. Verder zien wij dat bij opleidings- en trainingsvragen steeds vaker wordt gevraagd om een gespecialiseerde opleiding te verzorgen voor specifieke doelgroepen als OR, raad van toezicht, raadsleden, etc.
Op deze manier wordt hun kennisniveau op peil gebracht, zodat zij op een passende manier hun toezichthoudende of controlerende rol kunnen vervullen.

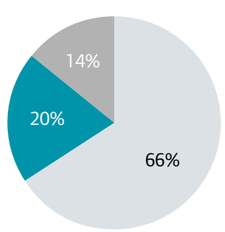
Vraag:

Als u klant zou zijn bij uw eigen organisatie, zou u dan vertrouwen hebben in de omgang met persoonsgegevens?





Geen bijzondere persoonsgegevens



Wel bijzondere persoonsgegevens

Deze vraag is nieuw in de Nationale Privacy Benchmark 2017 en is bewust als 'gewetensvraag' opgenomen. Nu iedere organisatie bezig is met het treffen van de nodige maatregelen is het voor mensen die daar een actief aandeel in hebben verleidelijk om te stellen dat men op de goede weg is. Hier wordt gevraagd vanuit het perspectief van de betrokkene te kijken naar de eigen organisatie.

Het goede nieuws is dat driekwart van de respondenten vertrouwen heeft in de eigen organisatie. Zorgpunt is dat een kwart van de respondenten dit vertrouwen niet heeft. En nog opvallender: de deelnemers die de eigen organisatie niet het vertrouwen geven blijken vrijwel allemaal te werken in omgevingen waar ook veel bijzondere persoonsgegevens worden verwerkt.

Hoe ver zijn organisaties met hun voorbereidingen op de AVG?

In deze sectie zijn de resultaten opgenomen van de vragen die bedoeld waren om te kijken waar organisaties staan met hun voorbereidingen op de AVG. Talrijke onderzoeken in 2017 geven aan dat organisaties nog niet klaar zijn, wat gezien de natuurlijke 'deadline' van 25 mei 2018 ook logisch is. Maar op welke punten ligt nog werk?

In de Nationale Privacy Benchmark 2017 zijn daarom specifieke verdiepingsvragen gesteld over:

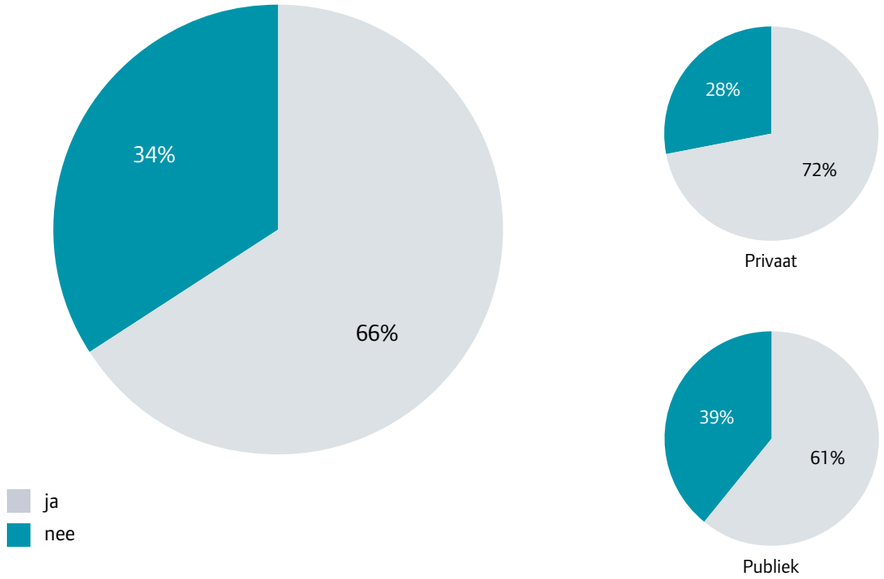
- Het beleggen van de rol van de Functionaris Gegevensbescherming (FG)
- Het krijgen van inzicht in verwerkingen en het vastleggen en beheren van dit inzicht in een register
- De kwaliteit van het protocol voor de melding van datalekken
- De afspraken met verwerkers over de omgang met persoonsgegevens
- Hoe men gebruik maakt van Privacy Impact Assessments (PIA's)
- Hoe men omgaat met de verplichting voor Privacy by Design (PbD)
- De kostenposten die men verwacht voor de komende periode
- Hoe men aan kennis komt omtrent de verplichtingen van de privacywetgeving

Algemeen beeld is dat de deelnemers uit de private sector steeds iets verder lijken te zijn dan de deelnemers uit de publieke sector. Een mogelijke verklaring is dat private ondernemingen zich meer realiseren dat een falen op privacy kan leiden tot een verlies aan klandizie. Dit geldt veel minder voor publieke ondernemingen. Daar is vaak geen sprake van concurrentie. Als betrokkene kan je immers je publieke dienstverlener niet kiezen.

Publieke organisaties realiseren zich hun verantwoordelijkheid, maar kennen hier blijkbaar net wat minder urgentie aan toe dan private ondernemingen.

Stelling:

We hebben de rol van de Functionaris Gegevensbescherming (FG) goed belegd

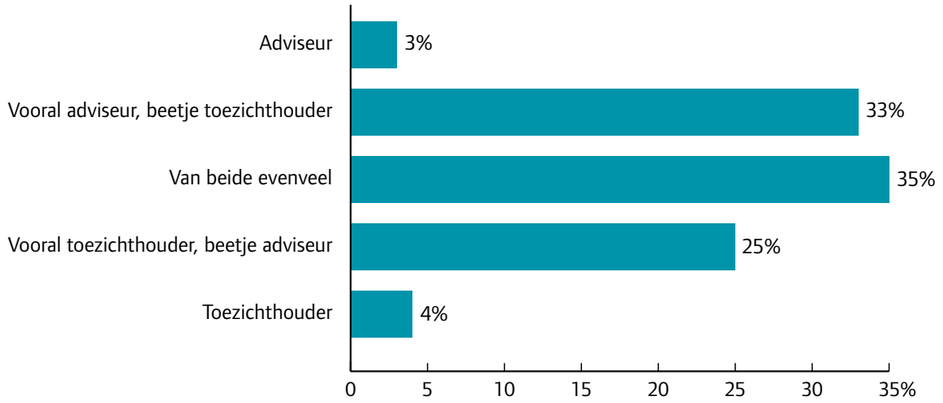


De rol van de FG is een veelbesproken onderdeel van de AVG. Wanneer moet je een FG aanstellen of wanneer is dit verstandig? En wat moet de FG dan precies doen, aan wie moet hij of zij zich verantwoorden? Gaan we zelf een FG aanstellen? Doen we dit samen of zoeken we een externe FG? Allemaal vragen die de afgelopen maanden in tal van organisaties zijn gesteld.

Tweederde van de respondenten geeft aan dat de rol van FG intussen goed is belegd. Hierbij valt wel op dat in de publieke sector dit percentage iets lager is. Juist omdat in de publieke sector een verplichting bestaat om een FG aan te stellen, terwijl dit in de private sector minder het geval is.

Stelling:

Een Functionaris Gegevensbescherming (FG) is vooral...



Een klassieke vraag die gegarandeerd discussie oproept tussen privacy officers tijdens congressen, opleidingen en bijeenkomsten is de vraag: wat is nu de rol van de privacy officer?

De beroepsgroep is op dit punt uitermate verdeeld. Zeker bij de respondenten in de publieke sector is de verdeeldheid groot. De private sector lijkt net iets meer te neigen naar de adviserende rol.

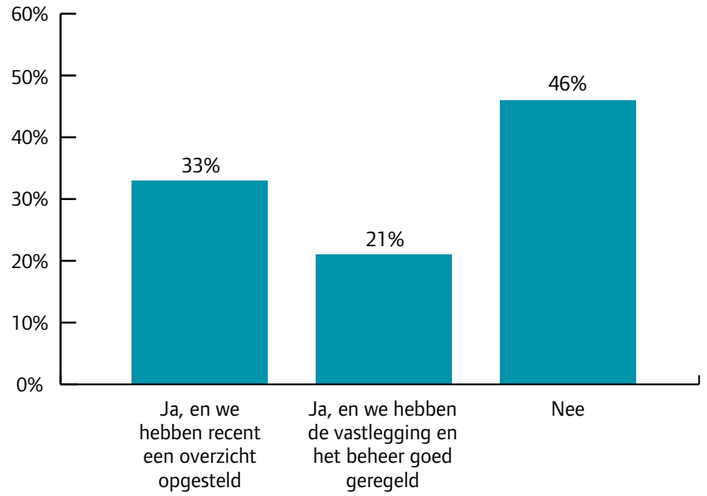
Organisaties hebben naar onze mening verschillende behoeften. Vanuit de wetgeving is de toezichthoudende rol van belang.

Inhoudelijk krijgt management meer behoefte aan advies op het gebied van privacy. Wat kan wel en wat kan niet. Het meedenken over deze vragen past echter veel meer bij een adviseur dan bij een toezichthouder.

Wij verwachten dat er een scherper onderscheid gaat ontstaan tussen de in de wet voorgestelde FG of 'data protection officer' (die duidelijke toezichthoudende taken heeft) en de privacy adviseur, die een organisatie helpt om met praktische vraagstukken om te gaan.

Stelling:

We beschikken over een passend register voor verwerkingen



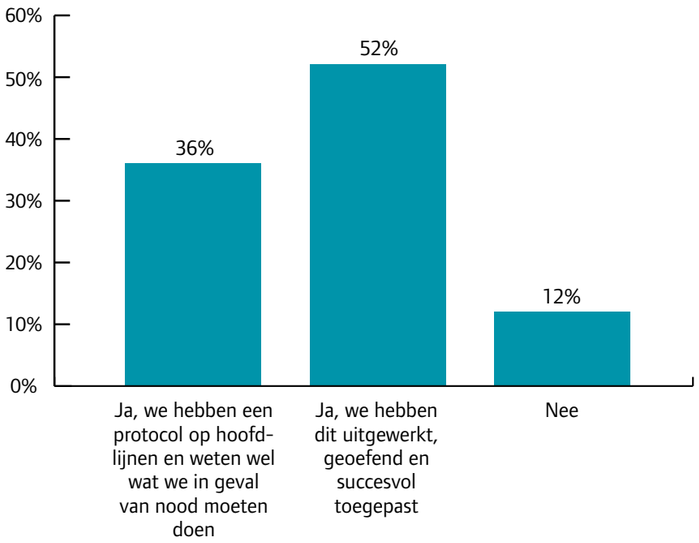
Voor veel organisaties is dit het startpunt van de AVG implementatie: het register dat inzicht geeft in de verwerkingen van persoonsgegevens.

Iets meer dan de helft van de respondenten is op weg of gereed. Bijna de helft van de respondenten is dit nog niet. De ervaring leert dat het opstellen van een register al de nodige hoofdbrekens vraagt: tot welk detailniveau moet je vastleggen, wanneer ben je volledig, doe je dit procesgericht of systeemgericht, et cetera.

Naar onze mening is de belangrijkste vraag: hoe blijft het verworven inzicht actueel. Het initieel aanleggen van een register is weliswaar al een mijlpaal, maar het beheer ervan en het toezicht op de actualiteit en de volledigheid bepaalt of aan de eisen van de privacy wetgeving is voldaan. Dit is bij 79% van de deelnemers nog onvoldoende ingeregeld.

Stelling:

We beschikken over een werkend protocol voor datalekken

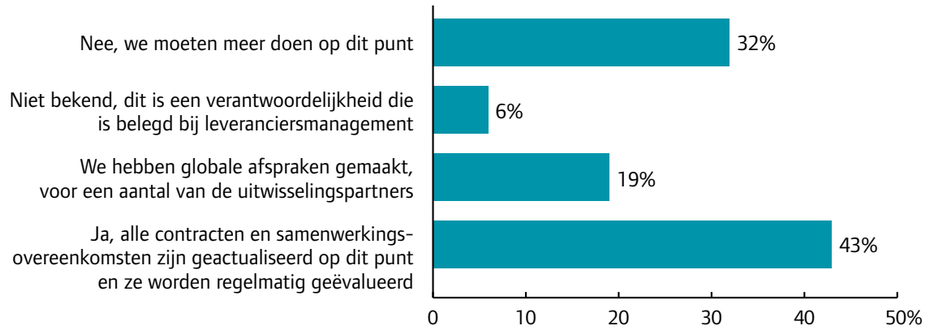


In Nederland is in 2016 al de nodige aandacht geweest voor de Meldplicht Datalekken. In dat kader hebben organisaties protocollen opgesteld voor de omgang met datalekken. Met deze protocollen is in 2017 de nodige ervaring opgedaan. Ruim de helft van de respondenten geeft aan dat de protocollen worden getoetst of in praktijk worden gebracht.

Deze maatregel lijkt daarmee het meest binnen organisaties geadopteerd. Desondanks heeft nog steeds 12% van de organisaties niets geregeld op dit punt.

Stelling:

We hebben sluitende afspraken gemaakt over de bescherming van persoonsgegevens met alle andere partijen met wie we persoonsgegevens uitwisselen en waarvoor we verantwoordelijk zijn



Om je organisatiedoelstellingen te halen en om efficiënt te opereren worden gegevens uitgewisseld met klanten, leveranciers en ketenpartners. Daarnaast zijn (delen van) bedrijfsprocessen uitbesteed bij derden.

In al deze uitwisselingsrelaties kunnen persoonsgegevens voorkomen, waarvoor u als organisatie wettelijk verant-woordelijk bent. De wet eist dat organisaties ‘in control’ zijn over de bescherming van persoonsgegevens waarvoor u verantwoordelijk bent, maar waarvan de bewerking is neergelegd bij een derde.

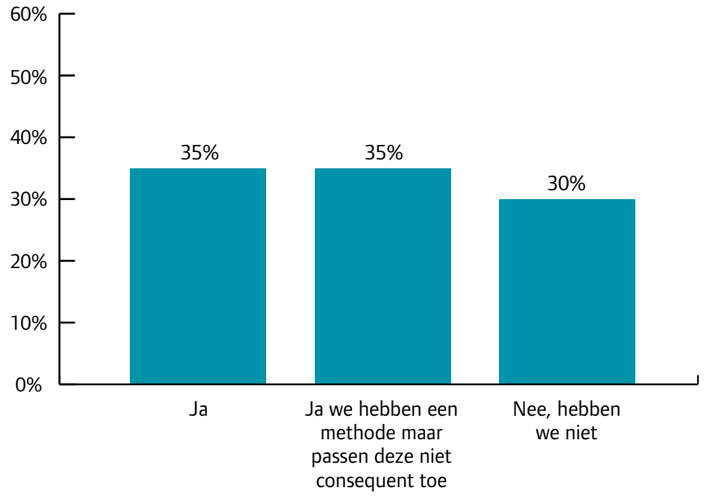
Dit vraagt om afspraken, en meer dan alleen globale afspraken. Hier geeft 43% aan dat dit aspect op orde is. Dit houdt in dat 57% op dit punt voor juni 2018 nog het nodige huiswerk heeft. Hier lijkt de publieke sector nog iets meer werk te hebben dan de private sector. Een mogelijke verklaring hiervoor is dat binnen de publieke sector veel gegevens worden uitgewisseld met ketenpartners. Het maken van goede afspraken over de bescherming van persoonsgegevens is binnen een (gelijkwaardige) ketenrelatie vaak lastiger dan in een traditionele klant-leveranciersrelatie.

In de praktijk is zichtbaar dat de hulp van de inkoopafdeling welkom is om tot de juiste afspraken te komen en bestaande afspraken te actualiseren.

Stelling:

We hebben een goede methode voor PIA's en passen deze consequent toe

(meerdere antwoorden mogelijk)



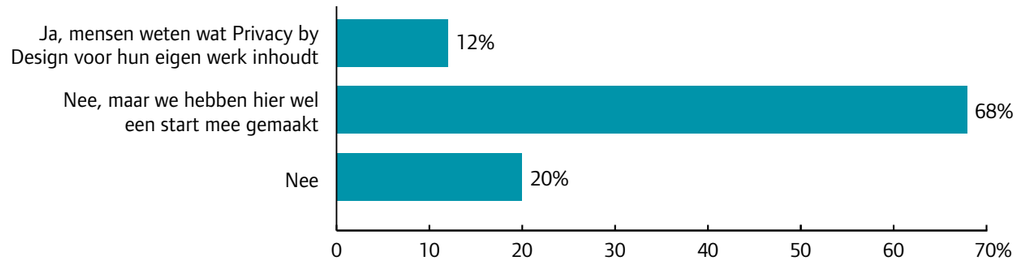
De PIA is al een gevleugelde term in privacy land. De verplichting om een Privacy Impact Assessment uit te voeren is een veelgehoord actiepunt. Desondanks heeft net een derde van de respondenten een PIA methode die men ook consequent toepast. Nog een derde heeft wel een methode, maar past deze nog niet consequent toe (dit komt binnen de publieke organisatie vaker voor dan binnen private organisaties). Bijna een derde beschikt nog niet over een PIA methode.

Op dit vlak is nog het nodige werk te doen. Dit is verklaarbaar omdat er niet zoiets bestaat als één soort PIA. Er is geen vaste vragenlijst, aanpak of resultaat voor een PIA.

Vanuit het Rijk en vanuit beroepsgroepen zijn er wel best practices verschenen, maar deze zijn niet zomaar klaar voor praktische toepassing. Een PIA moet vaak pragmatisch zijn, flexibel en inhoudelijk relevant. De bestaande best practices verdienen op dit punt nog verdere gewenning en ontwikkeling.

Stelling:

We hebben consequent Privacy by Design ingericht binnen de hele organisatie



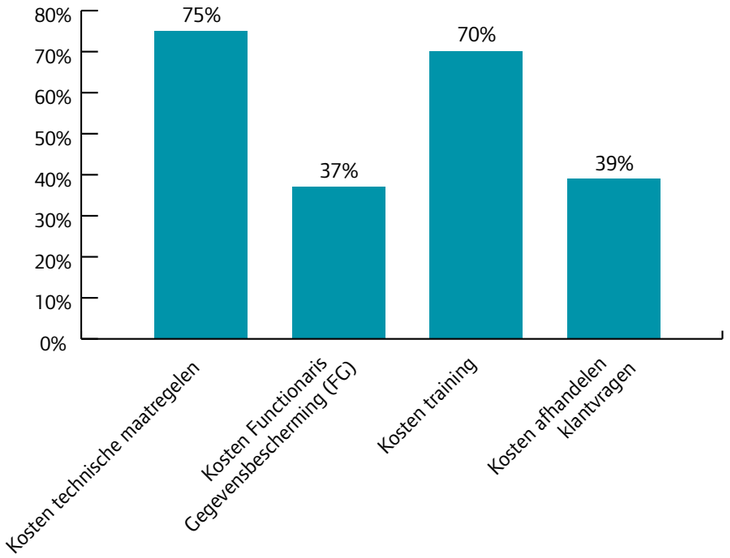
Een van de meest veelbelovende aandachtspunten uit de AVG is Privacy by Design. Privacy by Design leert allereerst om na te denken over verstandig gebruik van persoonsgegevens: welke gegevens zijn echt nodig en waar gebruik ik ze voor. Daarna kan de vraag worden gesteld hoe deze gegevens passend kunnen worden beschermd.

De relatieve nieuwheid van dit punt, alsmede het open karakter van de norm (wat is het precies, wanneer doe je het goed) lijkt ervoor te zorgen dat nog niet zoveel organisaties hier raad mee weten.

Een kleine minderheid geeft aan dat de mensen binnen hun organisatie weten wat Privacy by Design voor hen inhoudt. De private sector lijkt op dit punt een kleine voorsprong te hebben op de publieke sector.

Vraag:

Voor welke posten verwacht u de komende jaren meer budget nodig te hebben?



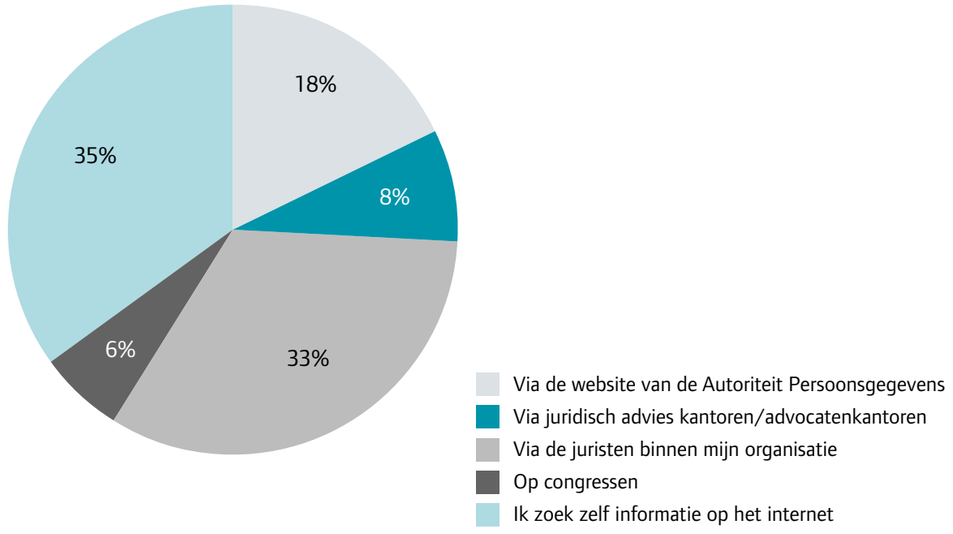
De respondenten verwachten dat met name de kosten die gemoeid zijn met technische beveiliging (75%) en met de trainingen voor medewerkers (70%) zullen toenemen.

Een kleine minderheid van de respondenten verwacht dat de kosten voor de FG nog zullen toenemen. We vermoeden dat dit samenhangt met het feit dat meer organisaties inmiddels al over een FG beschikken. Ten slotte verwacht een kleine minderheid van de respondenten dat de kosten voor de afhandeling van klantvragen zullen toenemen.

Op zichzelf zal het afhandelen van rechten van betrokkenen (denk aan inzage/correctie/verwijdering) de nodige tijd gaan vragen van organisaties. Blijkbaar gaat een meerderheid van de respondenten ervan uit dat deze verzoeken vanuit de reguliere lijncapaciteit zullen worden afgehandeld.

Vraag:

Hoe komt u aan informatie over de geldende regels omtrent privacy?



De privacywetgeving is door haar open normering niet eenvoudig te doorgronden. Daarom is in de NPB 2017 de vraag gesteld hoe men aan de relevante informatie komt. Het beeld daarbij is vrij divers. Zo'n 18% vertrouwt op de informatievoorziening vanuit de AP. Een derde raadpleegt het liefst de jurist uit de eigen organisatie.

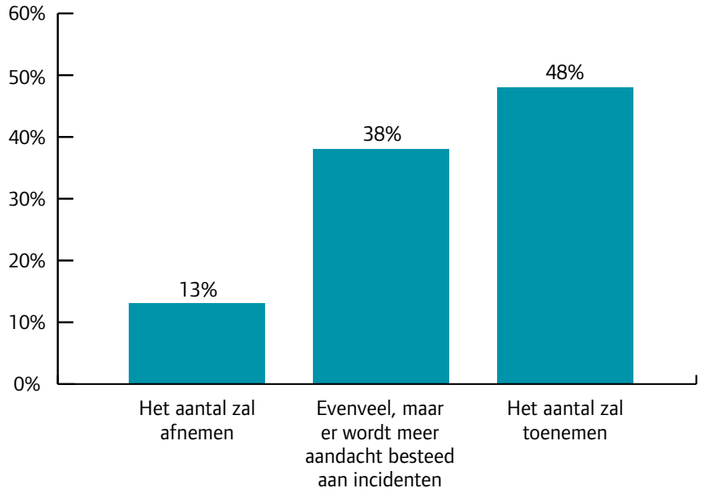
Opvallend en risicovol vinden wij dat het grootste deel van de respondenten aangeeft dat men zelf op zoek gaat naar informatie op het internet. Blijkbaar wordt dit gezien als een goede inspiratiebron, tenzij er toch wel degelijk beperkingen zijn aan de kwaliteit van deze informatie:

- **Is de informatie actueel** - regelmatig wordt in artikelen gerefereerd aan eerdere (concept) versies van de Europese wetgeving. Het is raadzaam om sowieso alle artikelen die vóór januari 2016 zijn geschreven over de AVG goed te controleren op actualiteit.
- **Is de informatie onafhankelijk** - leveranciers van producten en diensten overgieten hun producten vaak met een GDPR of AVG sausje om een graantje mee te pikken van de toegenomen aandacht.
- **Is de informatie van toepassing op mijn context** - bepaalde inschattingen van wat wel mag en wat niet kunnen voor de ene organisatie geldig zijn en voor de andere niet. De eisen die men stelt aan het gebruik van persoonsgegevens zijn vaak context afhankelijk. Het raadplegen van internetbronnen zonder zich te verdiepen in de context kan daarom leiden tot verkeerde interpretaties.

De toekomst

Vraag:

Wat is uw verwachting voor de ontwikkeling van het aantal datalekken of privacy incidenten de komende jaren?



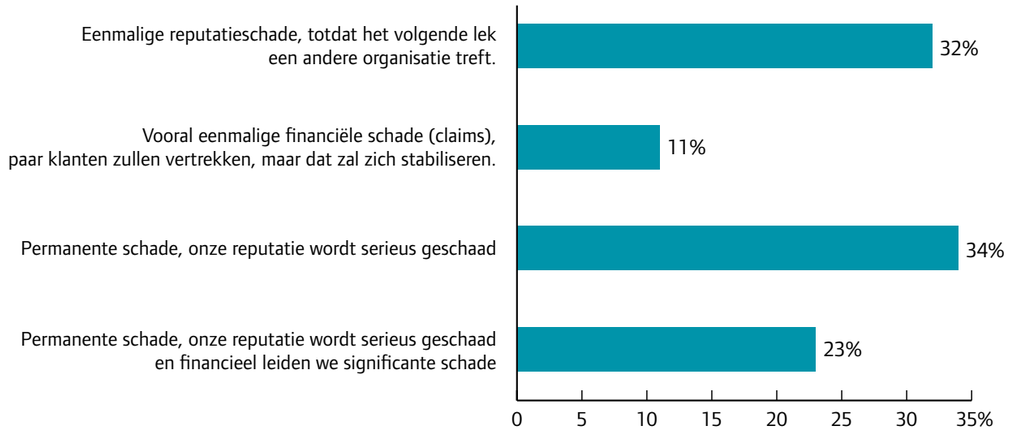
Met de Wet Meldplicht Datalekken is een nieuw begrip geïntroduceerd: een datalek. In het verleden bestonden er ook al incidenten, maar deze werden nog geen datalek genoemd.

Het begrip ‘datalek’ is intussen ook in de media ingeburgerd. De artikelen over datalekken, het ontstaan ervan en de consequenties voor de veroorzakers en verantwoordelijken worden talrijker.

De vraag is, of men verwacht dat zich meer beveiligingsincidenten of inbraken gaan voordoen. De respondenten geven overwegend (48%) aan dat het aantal gaat toenemen. Daarnaast geeft 38% aan dat zij niet verwachten dat er meer inbreuken gaan zijn, maar geven wel aan dat de inbreuken (door de grotere kans op openbaarmaking) meer publiciteit zullen krijgen.

Vraag:

Stel: uw organisatie komt in het nieuws omdat persoonsgegevens via uw organisatie onbedoeld openbaar zijn geworden. Hierdoor kan identiteitsfraude plaatsvinden. Hoe schat u de ‘schade’ in?



Het bepalen van de schade van een datalek is om twee redenen een interessante vraag:

1. De boetes zijn recent verhoogd en dit criterium wordt te pas en te onpas gebruikt als argument om privacy hoger op de agenda te krijgen.
2. De schade van een datalek is uiterst lastig te calculeren. Centraal in de discussie staat vaak de ‘reputatieschade’ en de waarde die daaraan moet worden toegekend.

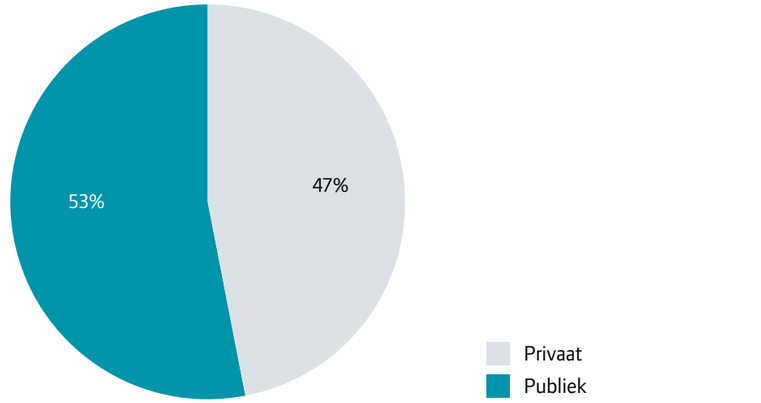
In 2017 verwacht 32% dat er wel sprake is van reputatieschade, maar dat dit wel overwaait zodra er een ander geval in de media komt.

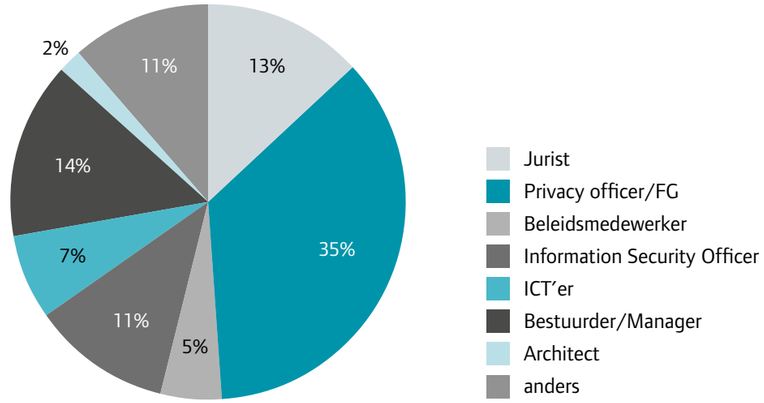
Belangrijkste wijziging ten opzichte van 2016 is dat deelnemers verwachten dat er sprake kan gaan zijn van serieuze financiële schade. Dit percentage stijgt van 8% in 2016 naar 23% in 2017. Het ligt voor de hand dat hier de boete-bedragen een rol spelen.

Over de deelnemers

Aan de benchmark hebben 97 deelnemers meegewerkt. De respondenten werkten volledig anoniem mee. Van de 97 deelnemers werkt 47% in de private sector en 53% in de publieke sector.

Het verzoek tot deelname aan de Nationale Privacy Benchmark 2017 is breed uitgezet. Een beeld van de achtergrond van de respondenten is hieronder opgenomen.





Over VKA

Een Privacy Officer van VKA biedt meer dan alleen compliancy. Wij voelen de verantwoordelijkheid om het vertrouwen van uw stakeholders te winnen en behouden. Zo kan uw organisatie blijvend functioneren in een data-gedreven maatschappij, en bent u ook daadwerkelijk in staat om de vruchten te plukken van nieuwe kansen die voortkomen uit ontwikkelingen zoals Big Data of Internet of Things.

VKA helpt bij bijvoorbeeld:

- Opzetten en uitvoeren van een project of programma om te voldoen aan de naderende privacy wetgeving.
- In beeld krijgen van de belangrijkste privacy risico's van uw organisatie en het uitvoeren van Privacy Impact Assessment (PIA).
- Vertalen van de abstracte privacy eisen naar concrete invulling binnen processen en ICT (hoe kom ik tot 'adequate gegevensbescherming', hoe geef ik inhoud aan bijvoorbeeld 'Privacy by Design' en 'Privacy Enhancing Technologies').
- Opzetten en implementeren van privacy awareness programma's en het geven van cursussen en het uitvoeren van oefeningen.

Over ECP

ECP | Platform voor de InformatieSamenleving is een onafhankelijk en neutraal platform waar overheid, bedrijfsleven en maatschappelijke organisaties samenwerken en kennis uitwisselen over de impact op en verantwoorde toepassing van nieuwe technologieën in de Nederlandse samenleving. Diverse activiteiten verbinden partijen en helpen de maatschappelijke en economische betekenis van ICT vorm te geven voor overheid, politiek en bedrijfsleven. Zo realiseert het platform doorbraken en creëert het de juiste randvoorwaarden voor een kansrijke en betrouwbare digitale samenleving. Bezoek **www.ecp.nl/activiteiten** voor een overzicht van onze projecten.

VERDONCK
KLOOSTER &
ASSOCIATES

ECP

Platform voor de
InformatieSamenleving