Privacy Governance onderzoek

Volwassenheid van privacybeheersing binnen Nederlandse organisaties

pwc

PwC Nederland juli 2019

www.pwc.nl/privacy

Inhoudsopgave

Introductie PwC Privacy Governance onderzoek 2019

Vanaf 2014 voert PwC jaarlijks een breed Privacy Governance onderzoek uit. Uit de onderzoeken in voorafgaande jaren is duidelijk geworden dat de Algemene Verordening Gegevensbescherming (AVG) een grote aanjager is geweest voor de toegenomen aandacht en inspanningen binnen organisaties op het gebied van privacy en omgang met persoonsgegevens.

Voor u ligt alweer het zesde door PwC uitgevoerde jaarlijkse onderzoeksrapport naar de volwassenheid van priacybeheersing binnen Nederlandse organisaties. Het belangrijkste verschil met de eerdere rapporten is uiteraard gelegen in het feit dat dit het eerste rapport is dat na de invoering van de AVG tot stand is gekomen. De focus in het onderhavige onderzoek ligt dus ook op de wijze waarop organisaties tot zover aan de verplichtingen uit de AVG invulling hebben gegeven, waar de knelpunten zitten en op welke deelgebieden de meeste inspanningen zijn verricht. Het onderzoeksrapport vormt als zodanig dus eeneerste ijkpunt nadat de AVG van toepassing is.

Gedurende de afgelopen jaren hebben we een goede indruk gekregen van de veelheid en verscheidenheid aan inspanningen die door organisaties in Nederland zijn verricht om compliant te worden aan de AVG-verplichtingen. Uit de resultaten van de opeenvolgende jaarlijkse Privacy Governance onderzoeken is gebleken dat het belang van privacy en zorgvuldige bescherming van persoonsgegevens steeds hoger op de agenda is komen te staan. We zien nog steeds een

www.pwc.nl/privacy

toename in het aantal organisaties dat de verantwoordelijkheid voor privacy en de verwerking van persoonsgegevens concreet belegt bij specifieke functies zoals een Data Protection Officer (DPO) of privacy functionarissen. Het aantal vacatures voor dergelijke specialistische functies neemt nog altijd toe. Gebrek aan adequate resources wordt door veel organisaties als één van de belangrijkste knelpunten gezien ten aanzien van AVG compliance.

Voor vrijwel alle organisaties zal het bereiken en handhaven van AVG compliance ook gedurende de komende jaren een belangrijk item blijven. Ook als er op dit vlak al grote inspanningen zijn verricht kan niet achterover worden geleund. Organisaties beseffen in toenemende mate dat AVG compliance ook naar de toekomst toe blijvende inspanningen vergt. Zo zal er continue aandacht blijven bestaan voor het creëren en op pijl houden van bewustwording van het belang van privacy en correcte omgang met persoonsgegevens. Grote uitdaging zal daarbij zijn om het beleid binnen verschillende afdelingen en groepsvennootschappen op elkaar af te stemmen en blijvend op elkaar aan te laten sluiten. Op dat punt ligt dus met name een grote uitdaging voor de privacy verantwoordelijken binnen organisaties waaronder de DPO's. Er zal dus veel van hen verwacht worden op het gebied van stakeholder management en het creëren van awareness. In veel gevallen is het nog altijd noodzakelijk om een cultuuromslag te bewerkstelligen en ingesleten bedrijfsprocessen en werkwijzen te doorbreken.

In het onderhavige onderzoek hebben we ook specifiek gekeken naar het gebruik van technologische hulpmiddelen bij het bereiken van AVG compliance. In hoeverre is het gebruik van tooling gangbaar en op welke gebieden wordt dit met name effectief ingezet? We zien dat bijna de helft van alle organisaties het afgelopen jaar investeringen heeft gedaan in het gebruik van op privacy en de verwerking van persoonsgegevens gerichte tools. Dat is een forse toename ten opzichte van vorig jaar toen dit voor minder dan 30% van de organisaties gold.

Verder duidt het gegeven dat een overgrote meerderheid (86%) van de organisaties aangeeft inmiddels procedures te hebben geïmplementeerd voor de afhandeling van rechten van betrokkenen (o.a. inzage- en correctieverzoeken en verzoeken om vergeten te worden) er op dat de verwachting bestaat dat individuen zich steeds meer bewust gaan worden van hun rechten en deze ook steeds vaker zullen effectueren.

Wat is het doel van het Privacy Governance onderzoek en hoe kan het uw organisatie helpen?

Het jaarlijkse Privacy Governance onderzoek van PwC geeft inzicht in de wijze waarop organisaties in Nederland omgaan met het onderwerp privacy, waarom ze het belangrijk vinden, hoe ze hierin investeren en op welke wijze ze omgaan met bestaande en nieuwe wet- en regelgeving. Dit onderzoek biedt de mogelijkheid om de staat van de privacy governance in de eigen organisatie te vergelijken met het algemene beeld bij organisaties in Nederland. Het rapport geeft geen oordeel over de privacy prestaties en compliance van individuele organisaties maar kan wel dienen als naslagwerk en als ijkpunt met betrekking tot de staat van privacy en data protectie.

Het Privacy Governance onderzoek verschaft een uniek beeld in de mate van volwassenheid van uw organisatie inzake de bescherming van persoonsgegevens in vergelijking met andere organisaties. Daarnaast geeft het weer in hoeverre organisaties in Nederland klaar zijn voor de nieuwe wet- en regelgeving uit de AVG. Dit rapport verschaft dus een duidelijk overzicht van de wijze waarop in Nederland wordt omgaan met het onderwerp privacy.

De toegevoegde waarde van het rapport voor u en uw organisatie bestaat onder meer uit:

- beter begrip van de aard en impact van nieuwe privacywetgeving;
- inzicht in de voor uw organisatie relevante privacyrisico's;
- vergroten van privacy bewustwording;
- evalueren van de privacy governance en resilience van uw eigen organisatie.

Wat zijn de verwachtingen op het gebied van handhaving door de Autoriteit Persoonsgegevens (AP)?

Uit de onderzoeken van de afgelopen jaren is naar voren gekomen dat de vrees voor boetes niet de voornaamste drijfveer voor organisaties is geweest om stappen richting AVG compliance te zetten. Toch kan niemand om de toegenomen bevoegdheden van de AP op dit gebied heen. Inmiddels worden de eerste boetes door de AP uitgedeeld en wordt het interessant om te zien op welke manier de hoogte van boetes wordt bepaald. Slaagt de AP erin om op dit punt transparant en consistent beleid te voeren? En in hoeverre spelen ontwikkelingen in internationaal verband hierbij een rol? Het valt te verwachten dat er binnen het samenwerkingsverband van Europese toezichthouders, de European Data Protection Board (EDPB), de nodige discussie zal ontstaan rondom het vaststellen van boetes. 'Daarbij is van belang dat één van de belangrijke doelstellingen van de AVG is om regelgeving binnen de EU verder op elkaar af te stemmen en te harmoniseren. Een geharmoniseerd en eenduidig uitgevoerd boetebeleid hoort daar zeker bij.

Security

In het onderhavige onderzoek hebben we de vraag gesteld welk onderdeel de meeste aandacht heeft gekregen bij het bereiken van AVG compliance. Opvallend is dat geen enkele organisatie informatiebeveiliging de hoogste prioriteit heeft gegeven. Toch is dit een zeer belangrijk aspect dat in toenemende mate van belang wordt bij het behouden van AVG compliance. Security incidenten en meer specifiek het veronachtzamen van verplichtingen op dit gebied zijn al aanleiding geweest voor Europese toezichthouders om zeer hoge boetes uit te delen die in specifieke gevallen ruim meer dan 100 miljoen euro bedragen. Het zal dus interessant worden om te zien of onder druk van dergelijke sancties informatiebeveiliging in de komende jaren bij een toenemend aantal organisaties de hoogste prioriteit zal krijgen.

Uitsplitsing van de resultaten

De afgelopen jaren hebben inmiddels ruim 1000 organisaties, uit verschillende sectoren en regio's, deelgenomen aan het PwC Privacy Governance onderzoek. De resultaten van ons onderzoek zijn ook dit jaar weer grafisch weergegeven in de volgende hoofdstukken:

- Privacy strategie en beleid
- Privacy incidenten en meldingen
- Uw organisatie en het privacyrisico
- Stellingen
- Over u en uw organisatie

Hoe de resultaten in te zetten voor uw eigen doeleinden

Op basis van het overall beeld zoals opgenomen in dit rapport adviseren wij om:

1. Dit rapport intern te bespreken met de privacy verantwoordelijken binnen uw organisatie. Dit stelt u in staat om de bestaande privacy governance structuur te verbeteren en te bepalen welke aspecten van AVG compliance verdere aandacht verdienen.
2. Belangrijke aspecten op basis van risico's en prioriteitsstelling te vertalen naar concrete actiepunten.
3. Periodiek de effectiviteit van de genomen maatregelen te meten en te kijken naar inzet van technologie (ook om de waarde van de privacy investeringen te verhogen).

Wij denken met dit onderzoek de Nederlandse privacy competenties als geheel te versterken en mede daardoor de Nederlandse concurrentie- en vertrouwenspositie op dit gebied in internationaal verband te verbeteren.

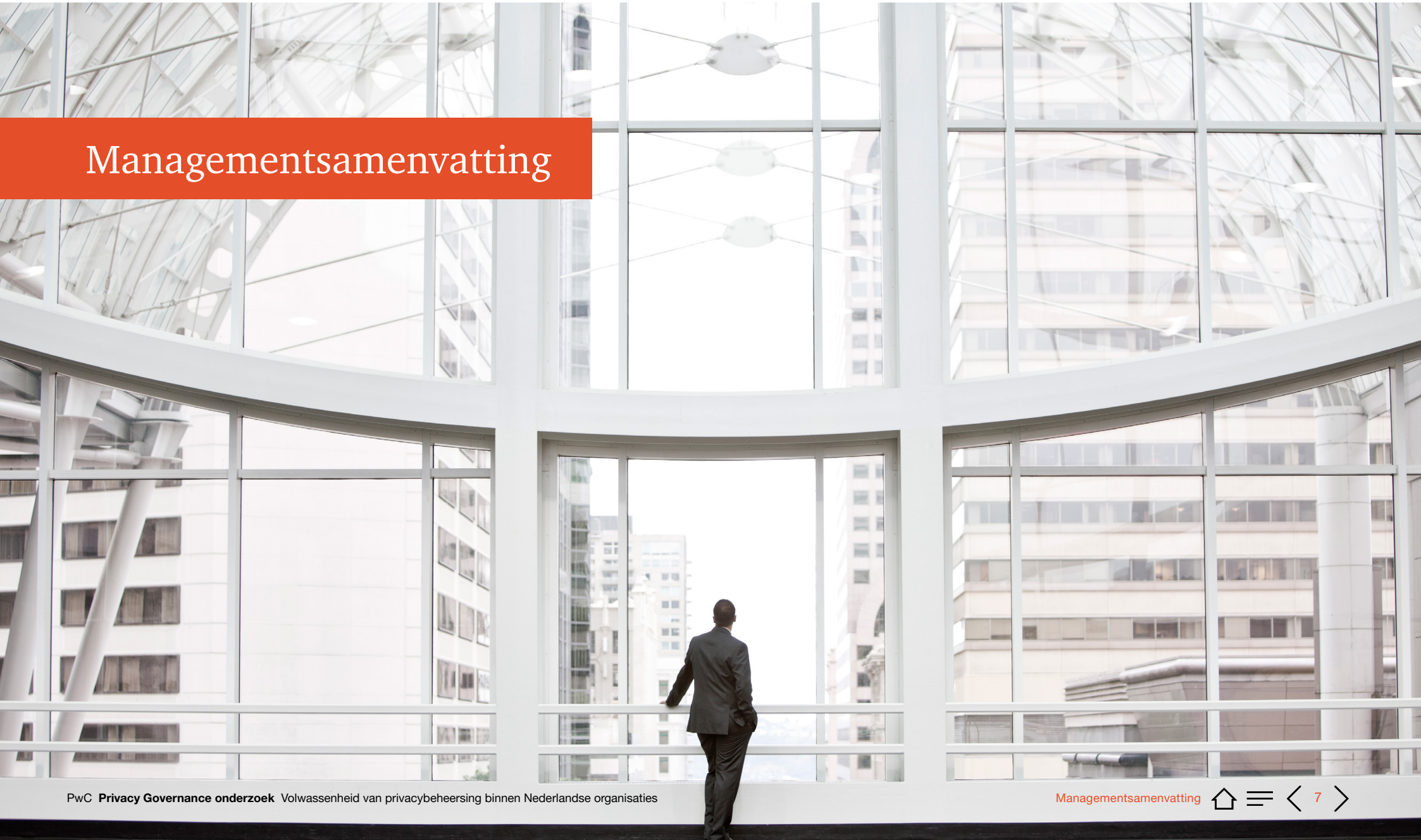
Het onderzoeksrapport verschaft daarnaast een algemeen beeld van de privacy aansturing binnen een groot aantal organisaties. Dit stelt u in staat op relevante punten een vergelijking te maken met de staat van de privacy governance structuur in uw eigen organisatie.

Wij zijn uiteraard graag bereid om de impact van deze rapportage nader met u te bespreken. We kunnen u daarnaast ondersteunen bij AVG gap assessments en bij het ontwikkelen van een actieplan dat is toegesneden op uw organisatie en zijn specifieke kenmerken en aandachtsgebieden.

Bram van Tiel
Partner Cybersecurity and Privacy
+31 (0) 88 792 53 88
bram.van.tiel@pwc.com

Yvette van Gemerden
Partner Legal
+31 (0) 88 792 54 42
yvette.van.gemerden@pwc.com

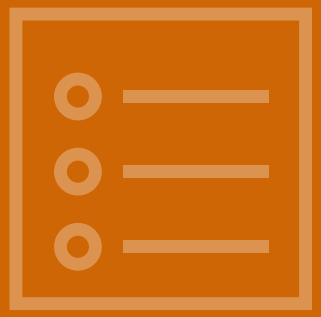
Managementsamenvatting



Managementsamenvatting

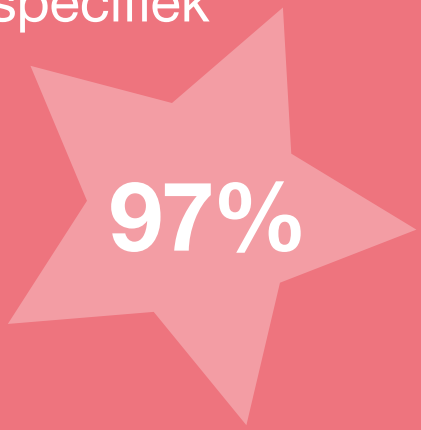
Ruime meerderheid van de organisaties heeft geen angst voor een onderzoek door de AP

Bij een eventueel onderzoek van de Autoriteit Persoonsgegevens zegt **89%** van de organisaties te verwachten voldoende compliant te zijn.



Verantwoordelijkheid voor privacy is door bijna alle organisaties specifiek belegd

97% van de organisaties geeft aan dat de verantwoordelijkheid voor het privacybeleid is belegd.



Meer organisaties doen extra investeringen in privacy

Bij **44%** van de organisaties zijn gedurende het afgelopen jaar extra investeringen gedaan op het gebied van privacy compliance en governance. Een verbetering ten opzichte van vorig jaar, toen maar bij **22%** van de organisaties extra investeringen waren gedaan.

Verwerkersovereenkomsten en technische en organisatorische maatregelen vormen nog knelpunten

Het sluiten van verwerkersovereenkomsten met andere partijen en het nemen van technische en organisatorische maatregelen om een passend beveiligingsniveau te waarborgen waren de grootste uitdagingen bij de implementatie van de AVG.

Managementsamenvatting

Privacy-by-design nog niet wijdverbreid geïmplementeerd

Maar liefst **88%** van de deelnemende organisaties houdt bij de ontwikkeling en implementatie van nieuwe systemen nog niet altijd rekening met de privacy van betrokkenen en de bescherming van persoonsgegevens.

88%

Procedures of richtlijnen voor rechten van betrokkenen worden geïmplementeerd

Een overgrote meerderheid **(86%)** van de organisaties geeft aan procedures te hebben voor afhandeling van rechten van betrokkenen. De kleine groep organisaties die dit nog niet heeft gedaan zegt hiermee bezig te zijn.

Onvoldoende mankracht en kennis vormt grootste bedreiging

Ruim een derde van de respondenten geeft aan dat ontbreken van mankracht of specialistische kennis het grootste struikelblok vormt voor borging van AVG compliance.

De helft van de organisaties investeert in technologie

Bijna **de helft** van alle organisaties heeft afgelopen jaar investeringen gedaan in het gebruik van tools.

Dat is een forse toename ten opzichte van vorig jaar toen dit voor minder dan **30%** van de organisaties gold.

Data Protection Impact Assessments (DPIAs) worden veelvuldig uitgevoerd

Alle organisaties geven aan inmiddels met regelmaat risicoanalyses (zoals Data Protection Impact Assessments) uit te voeren. Vorig jaar deed slechts **33%** van de organisaties dit. Een teken dat organisaties privacy compliance hogere prioriteit hebben gegeven.

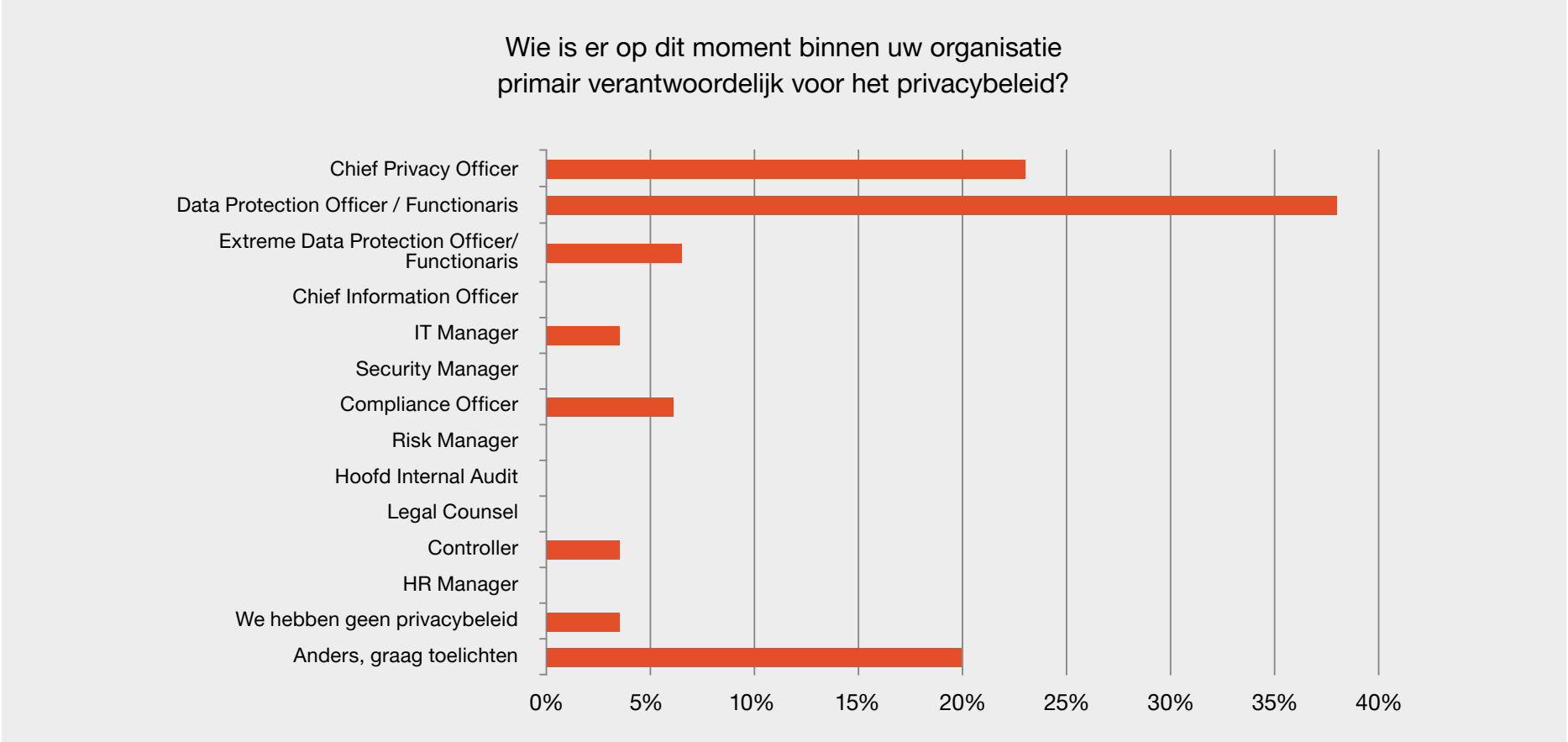
100%

Resultaten

Privacy strategie en beleid

Het privacybeleid kan door organisaties op verschillende manieren worden ingevuld. Met **37%** kiezen de meeste organisaties voor het aanstellen van een Data Protection Officer (of Functionaris voor de Gegevensbescherming). Een aanzienlijke groei ten opzichte van vorig jaar, toen **16%** van de organisaties een dergelijke functie hadden belegd.

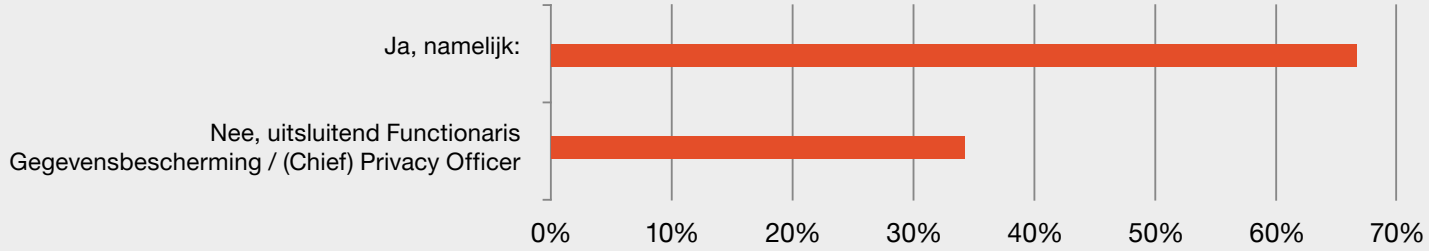
Slechts **3%** van de organisaties geeft aan dat de verantwoordelijkheid voor het privacybeleid niet is belegd of dat er geen sprake is van privacybeleid. Een enorme verbetering ten opzichte van vorig jaar, toen **23%** van de organisaties aangaf de verantwoordelijkheid voor het privacybeleid niet te hebben belegd of er in het geheel geen sprake was van een privacybeleid.



Privacy strategie en beleid

Bij de meerderheid van de organisaties **(66%)** heeft de Functionaris Gegevensbescherming naast zijn taak als FG nog een andere functie.

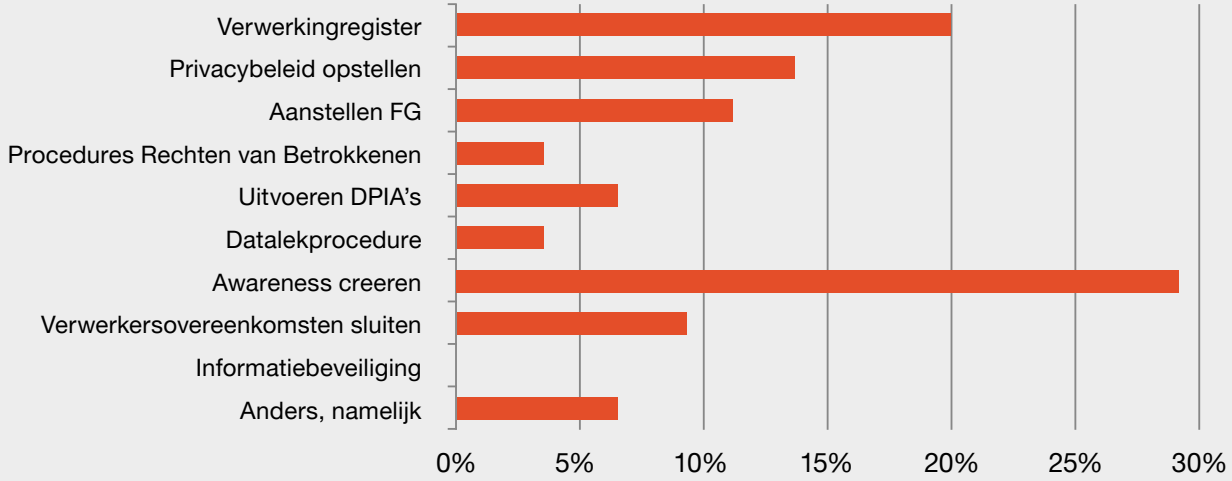
Heeft de Functionaris Gegevensbescherming / (Chief) Privacy Officer nog een andere functie?



Privacy strategie en beleid

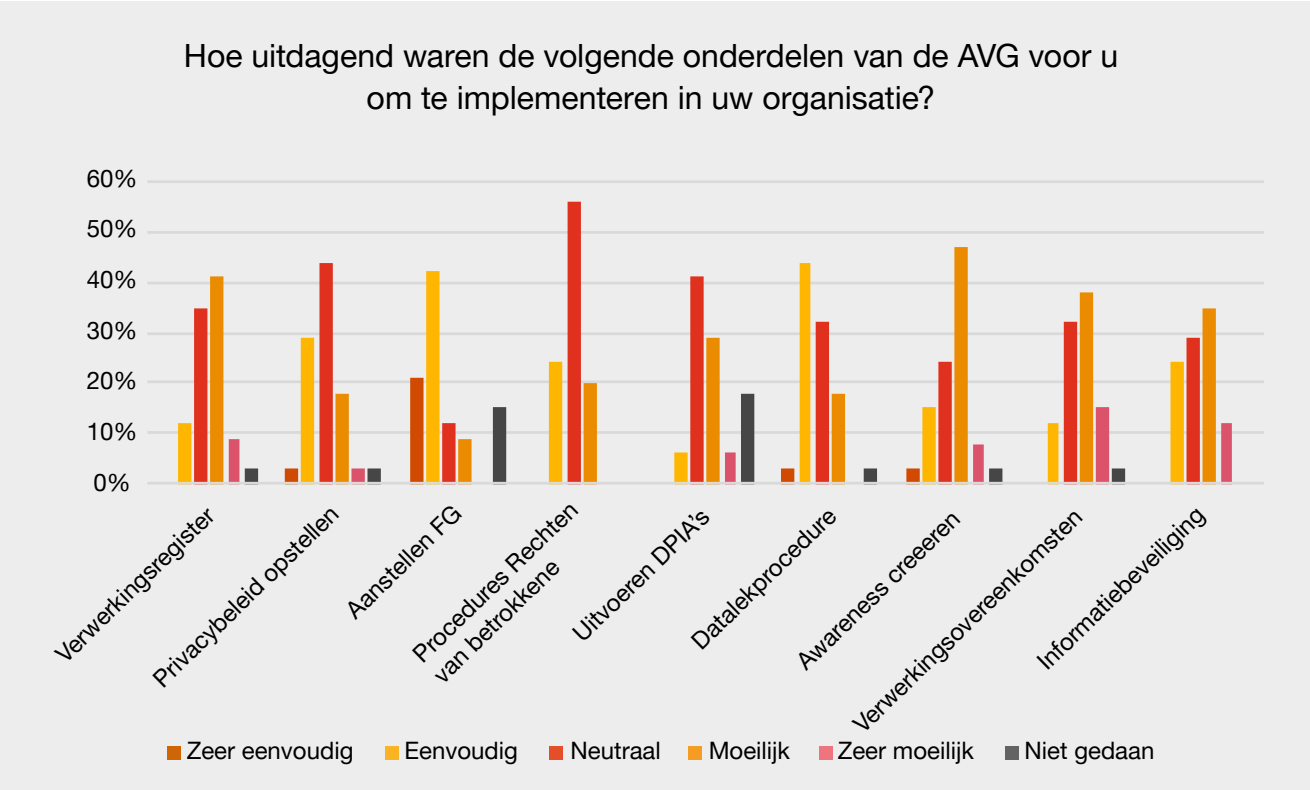
Bij de meeste organisaties **(29%)** is het creëren van awareness binnen de organisatie de hoogste prioriteit geweest bij de implementatie van de AVG. Opvallend is dat geen enkele organisatie informatiebeveiliging de hoogste prioriteit heeft gegeven.

Wat heeft bij uw organisatie de meeste prioriteit gehad bij de implementatie van de AVG?



Privacy strategie en beleid

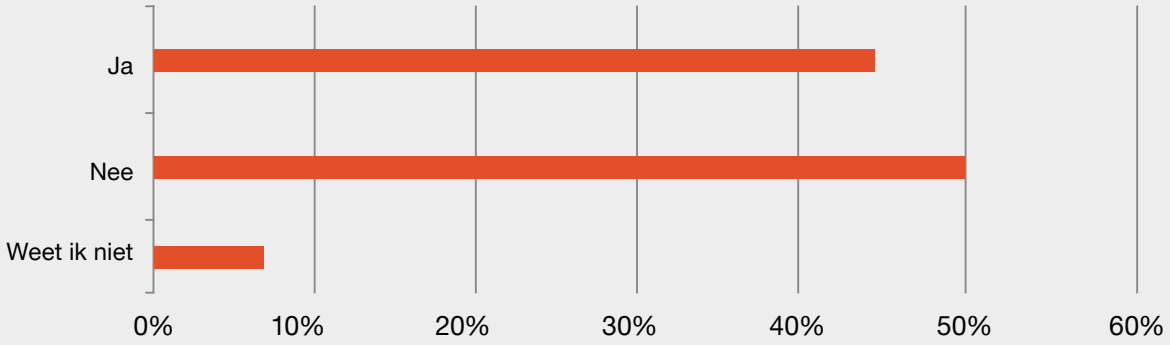
Het sluiten van verwerkersovereenkomsten met andere partijen en het nemen van technische en organisatorische maatregelen om een passend beveiligingsniveau te waarborgen waren de grootste uitdagingen bij de implementatie van de AVG. Ook het sluiten van verwerkingsovereenkomsten en het creëren van awareness binnen de organisatie werd als moeilijk ervaren. Het aanstellen van een Functionaris Gegevensbescherming werd daarentegen als relatief eenvoudig ervaren.



Privacy strategie en beleid

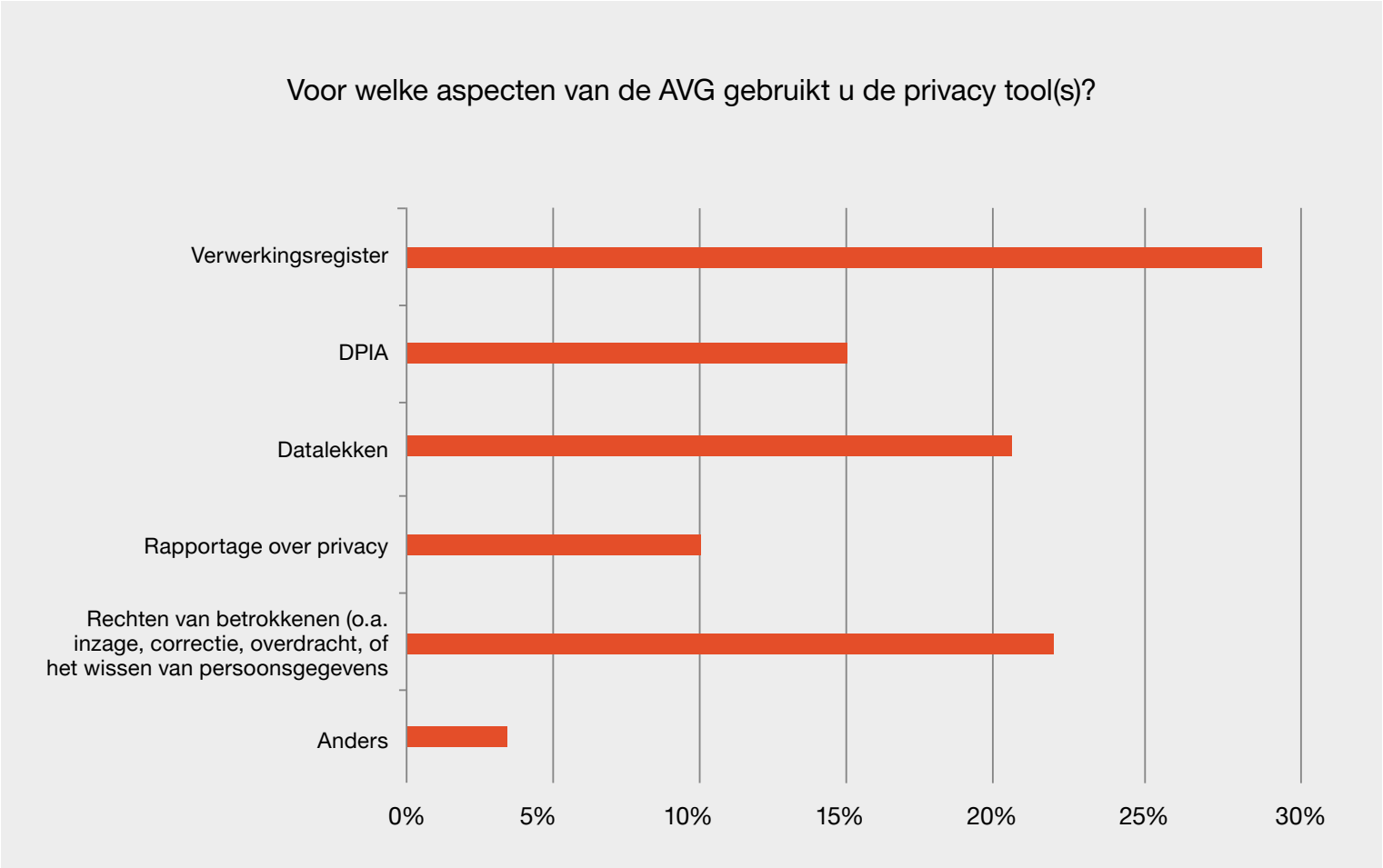
Bij **44%** van de organisaties zijn gedurende het afgelopen jaar extra investeringen gedaan op het gebied van privacy compliance en governance. Een verbetering ten opzichte van vorig jaar, toen maar bij **22%** van de organisaties extra investeringen waren gedaan.

Heeft uw organisatie het afgelopen jaar geinvesteerd in privacy tools?



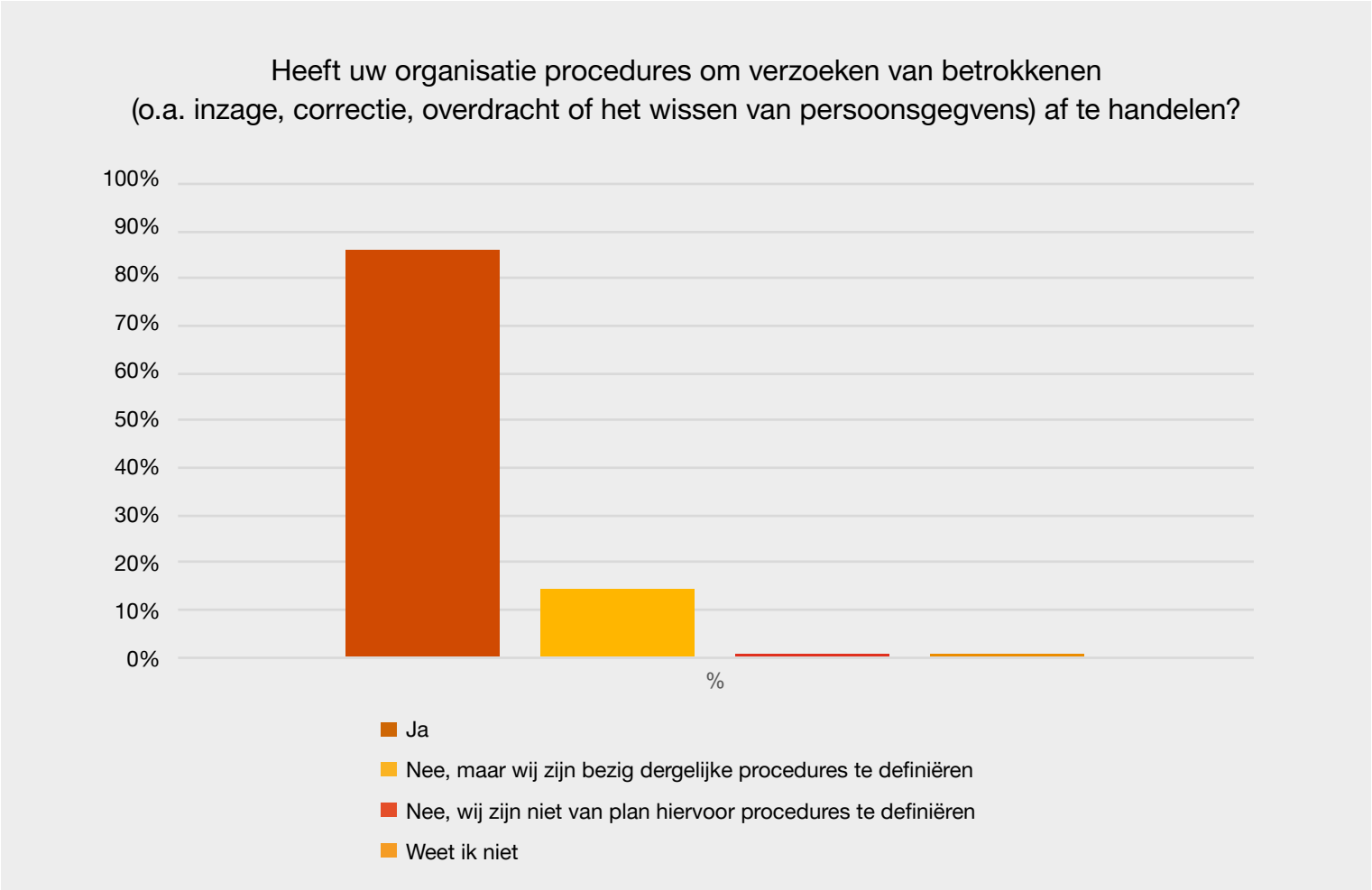
Privacy strategie en beleid

Privacy tools kunnen voor een verscheidenheid aan toepassingen worden gebruikt. Het vaakst **(28%)** gebruiken organisaties tools voor het beheer van het verwerkingsregister.



Privacy strategie en beleid

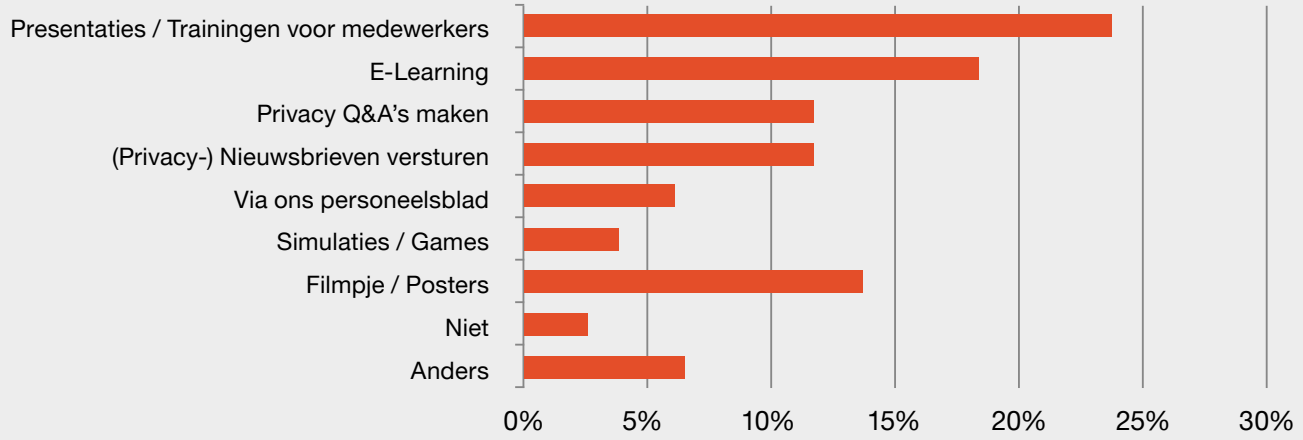
De overgrote meerderheid **(86%)** van de organisaties geeft aan procedures te hebben geïmplementeerd voor de afhandeling van inzage- en correctieverzoeken, verzoeken tot overdracht van gegevens of verzoeken om vergeten te worden. De kleine groep organisaties die dit nog niet heeft gedaan zegt hiermee bezig te zijn. Dit is van groot belang, omdat het hier gaat om een wettelijke verplichting.



Privacy strategie en beleid

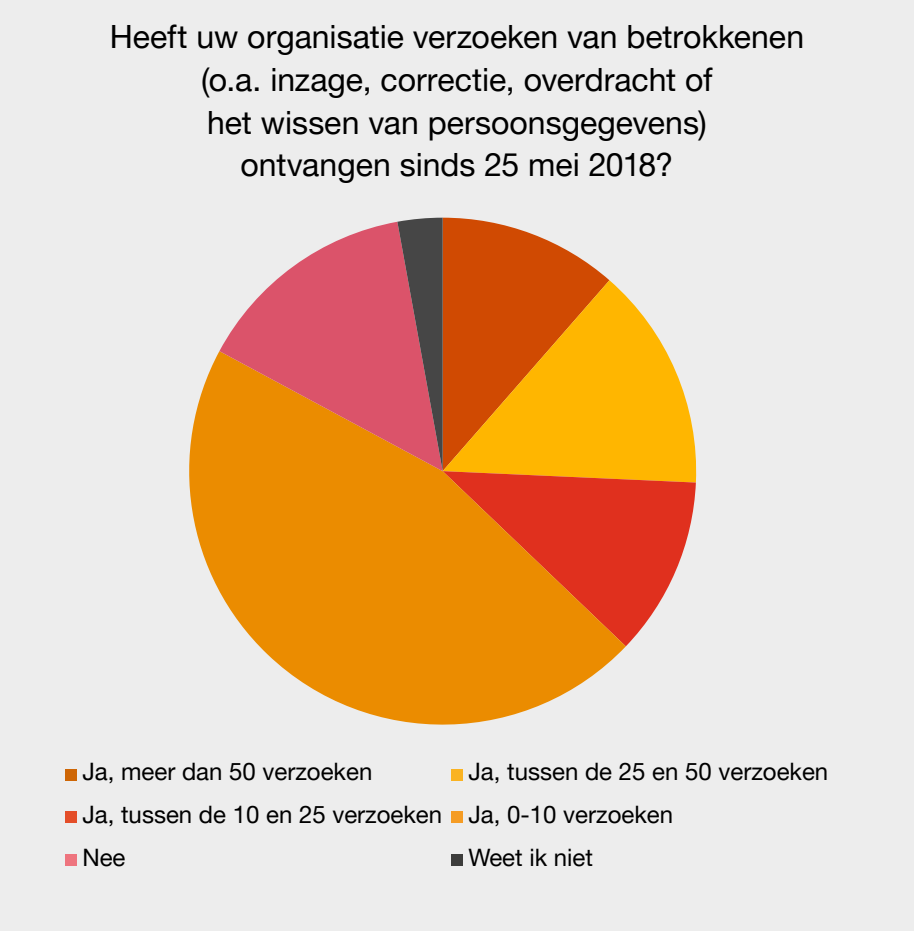
Privacy awareness heeft hoge prioriteit gehad bij bijna alle organisaties in het jaar van de inwerkingtreding van de AVG. Slechts **3%** van de organisaties doet op dit moment niet aan het verhogen van de privacy awareness. Ten opzichte van vorig jaar is dit een enorme verbetering, toen ruim een vijfde **(22%)** van de organisaties aangaf op dat moment niets te doen aan het verhogen van de privacy awareness. Het geven van medewerkerspresentaties is het populairste middel om het verhogen van de privacy awareness binnen de organisatie te bewerkstelligen.

Hoe heeft u vanaf 25 mei 2018 de privacy awareness binnen uw organisatie verhoogd?



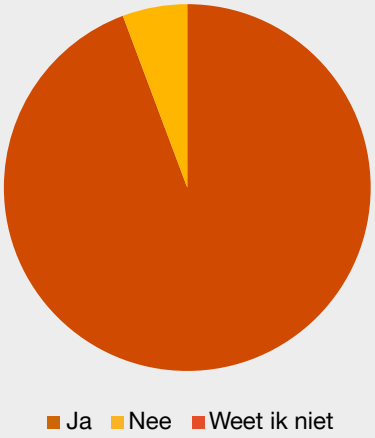
Privacy incidenten en meldingen

Slechts **14%** van de organisaties geeft aan nog geen verzoeken te hebben gehad van betrokkenen die hun rechten willen uitoefenen. Het gaat om verzoeken die betrokkenen aan organisaties kunnen doen wat betreft het gebruik van hun persoonsgegevens.

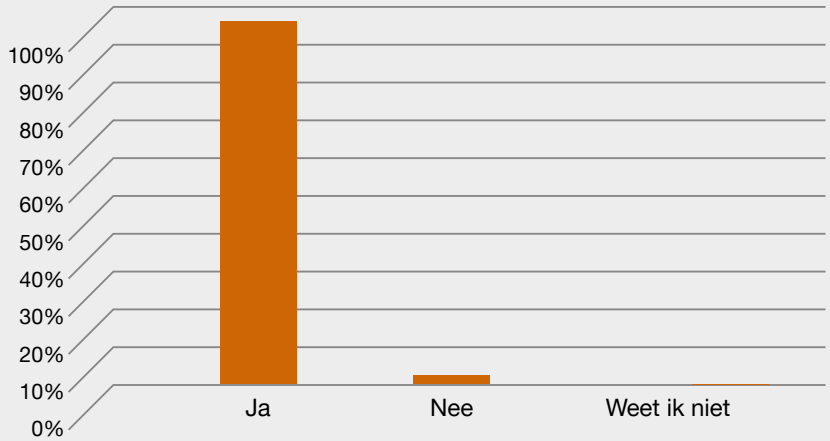


Privacy incidenten en meldingen

Heeft uw organisatie een procedure voor het omgaan met datalekken?



Houdt uw organisatie een overzicht bij van datalekken?



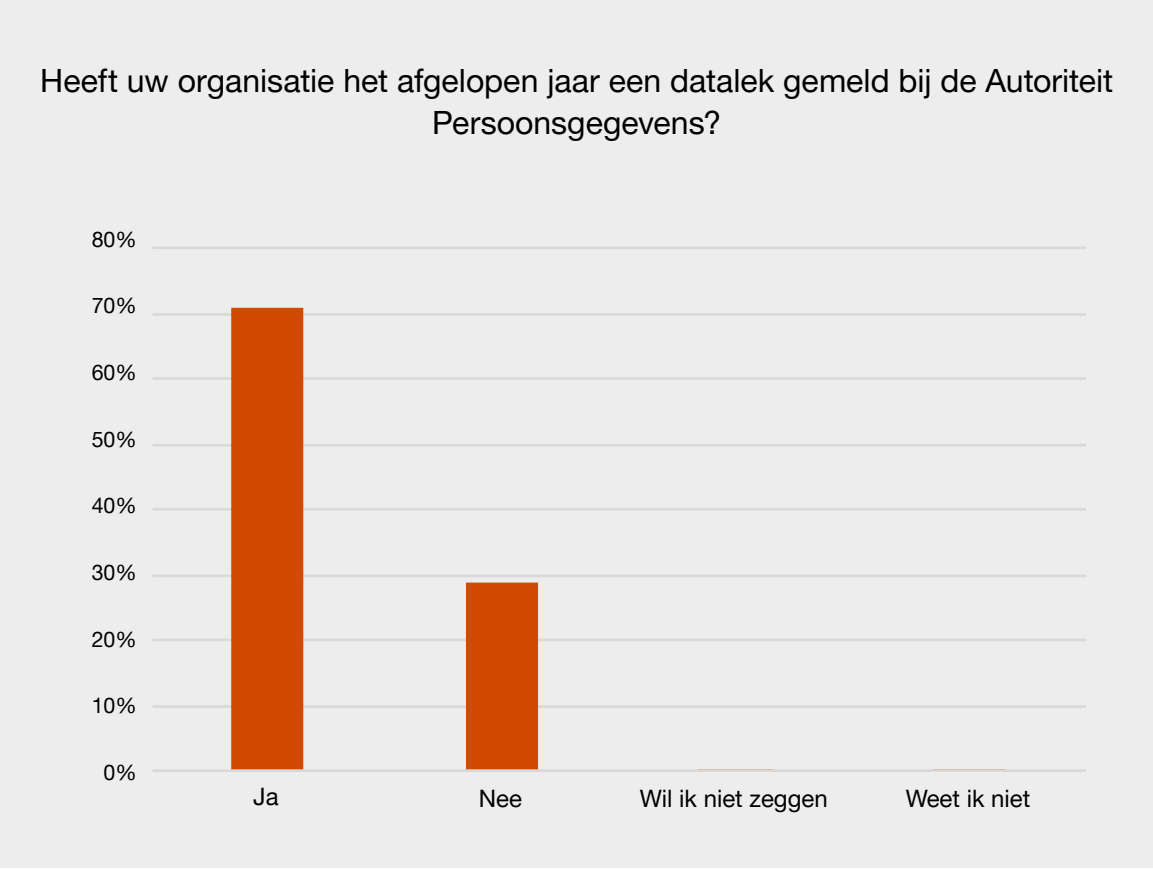
Vanaf 1 januari 2016 bestaat voor alle organisaties de verplichting om datalekken onverwijld te melden bij de Autoriteit Persoonsgegevens (AP) en in bepaalde gevallen ook betrokkenen hierover te informeren. Bij de melding moeten onder meer de impact van het datalek en de ter zake te nemen maatregelen worden vermeld.

Een kleine groep van de organisaties **(6%)** geeft aan nog helemaal geen procedure tot stand te hebben gebracht voor het omgaan met datalekken.

Bijna alle organisaties **(97%)** geven aan te voldoen aan de verplichting om een overzicht van datalekken bij te houden. Dit is een enorme verbetering ten opzichte van vorig jaar, toen **53%** van de organisaties aangaf te voldoen aan deze verplichting.

Privacy incidenten en meldingen

Bij **71%** van de organisaties hebben zich het afgelopen jaar één of meerdere datalekken voorgedaan die zijn gemeld bij de Autoriteit Persoonsgegevens.



Uw organisatie en het privacyrisico

Op basis van de Algemene Verordening Gegevensbescherming (AVG) is het verplicht om contractuele verplichtingen op te leggen aan externe partijen (bijv. leveranciers) die in uw opdracht persoonsgegevens verwerken. Als organisatie kunt u ervoor kiezen om deze verplichtingen in bestaande contracten te verwerken of separaat een verwerkersovereenkomst te sluiten.

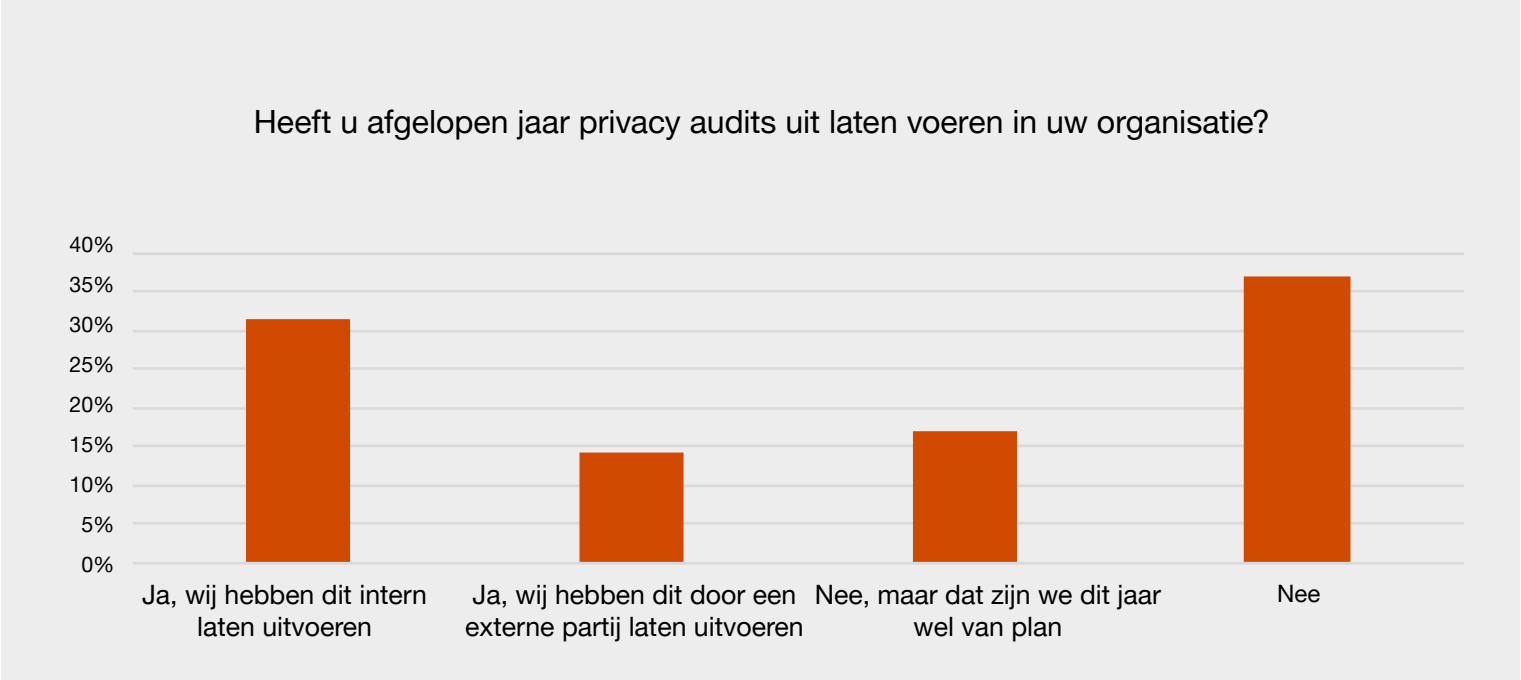
Door ongeveer **95%** van de organisaties worden contractuele verplichtingen met verwerkers van persoonsgegevens inderdaad vastgelegd in aparte verwerkersovereenkomsten of als onderdeel van het servicecontract. De overige organisaties laten geen persoonsgegevens door derden verwerken of zeggen geen contractuele verplichtingen op te leggen aan externe partijen.

Uw organisatie en het privacyrisico

Alle organisaties voeren met regelmaat risicoanalyses (zoals Data Protection Impact Assessments) uit. Vorig jaar deed slechts **33%** van de organisaties dit. Een teken dat organisaties privacy compliance hogere prioriteit hebben gegeven. Een derde van de organisaties geeft aan dat het uitvoeren van een DPIA een standard onderdeel is bij implementatie van alle nieuwe systemen, programma's en processen.

Uw organisatie en het privacyrisico

Bijna de helft **(45%)** van de organisaties geeft aan dat zij dit jaar privacy audits hebben laten uitvoeren en **17%** zegt dat dit jaar van plan te zijn.



Stellingen

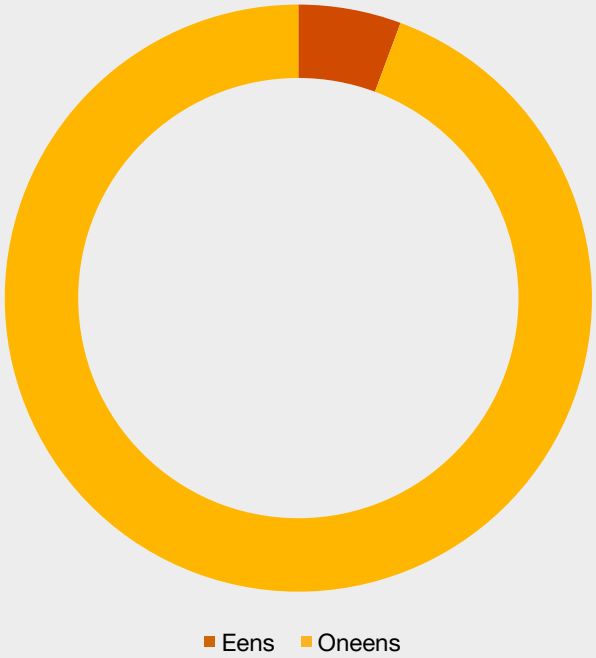
Het overgrote merendeel **(88%)** van de respondenten geeft aan dat de AVG de organisatie heeft aangespoord om meer grip te krijgen op het verwerken van persoonsgegevens.

Stellingen

Op basis van de AVG ishet verplicht om bij de ontwikkeling en implementatie van nieuwe systemen rekening te houden met de privacy van betrokkenen en de bescherming van persoonsgegevens.

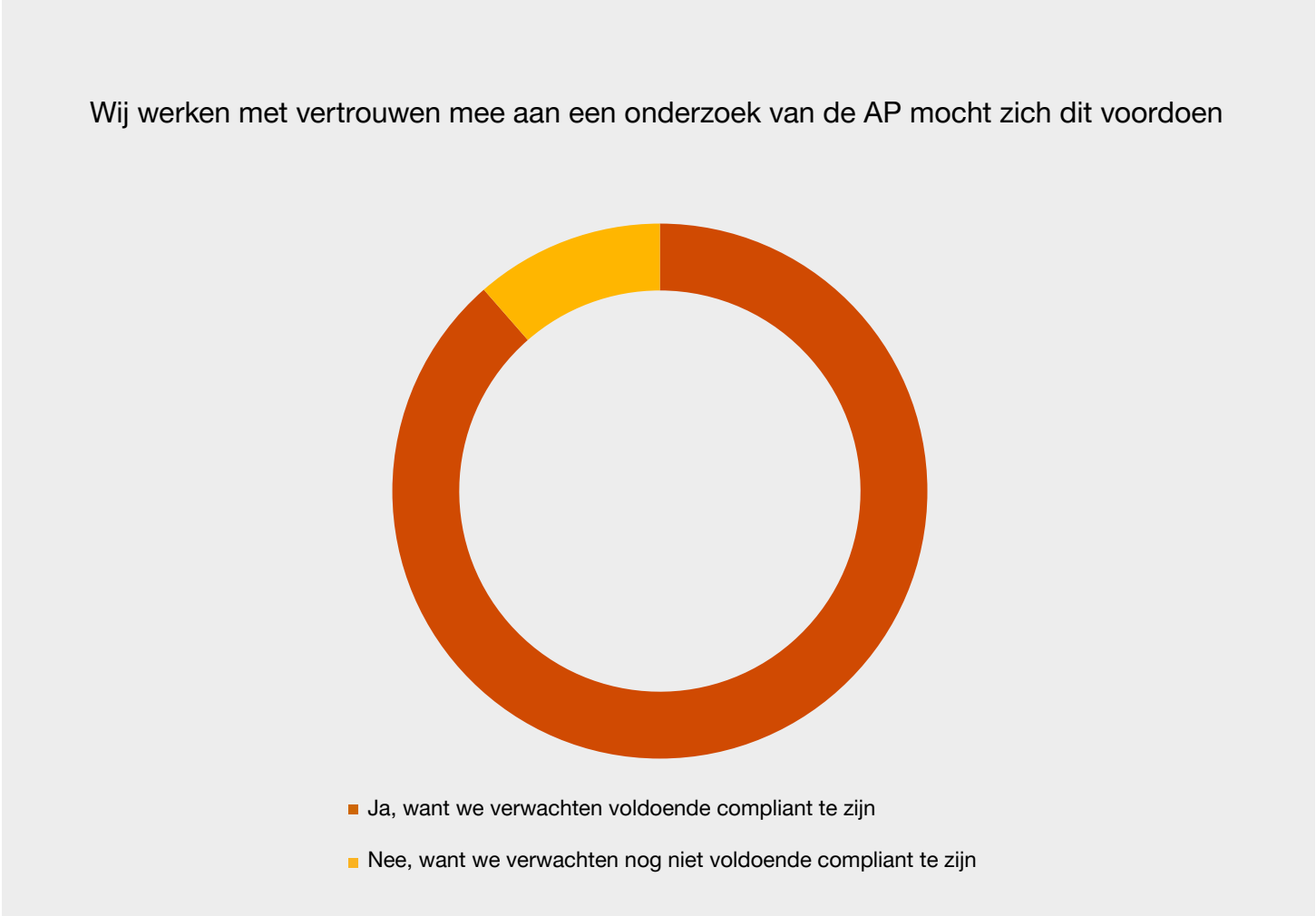
Ondanks deze verplichting geeft **88%** van de deelnemende organisaties aan hier bij de ontwikkeling van nieuwe systemen nog niet altijd rekening mee te houden.

Bij implementatie van nieuwe systemen houden wij altijd in een vroeg stadium rekening met privacyaspecten en de bescherming van persoonsgegevens
(Privacy by Design & Privacy by Default principes)



Stellingen

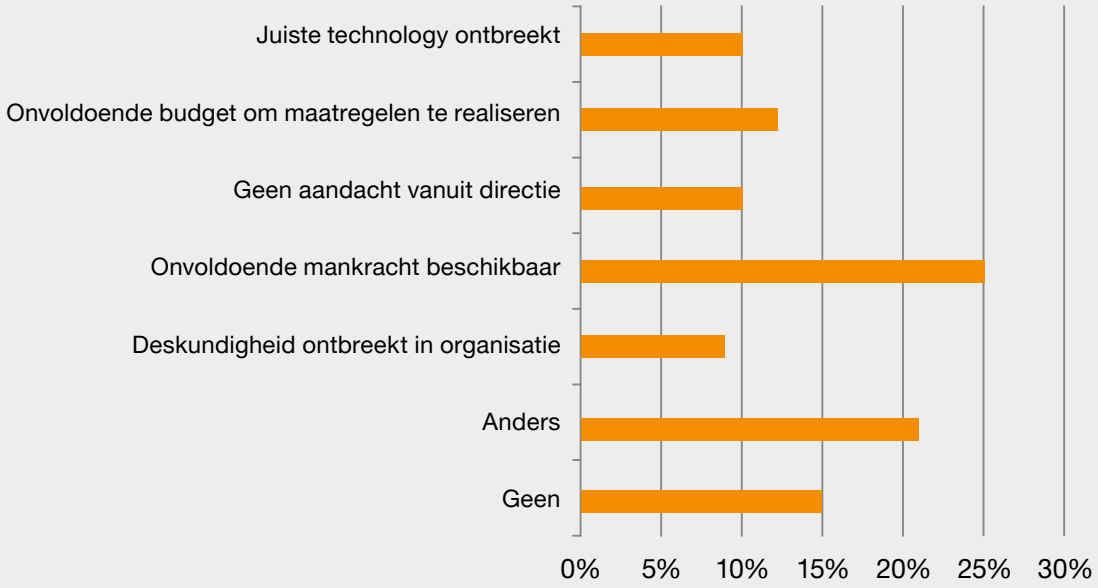
Bij een eventueel onderzoek van de Autoriteit Persoonsgegevens zegt **89%** van de organisaties te verwachten voldoende compliant te zijn.



Stellingen

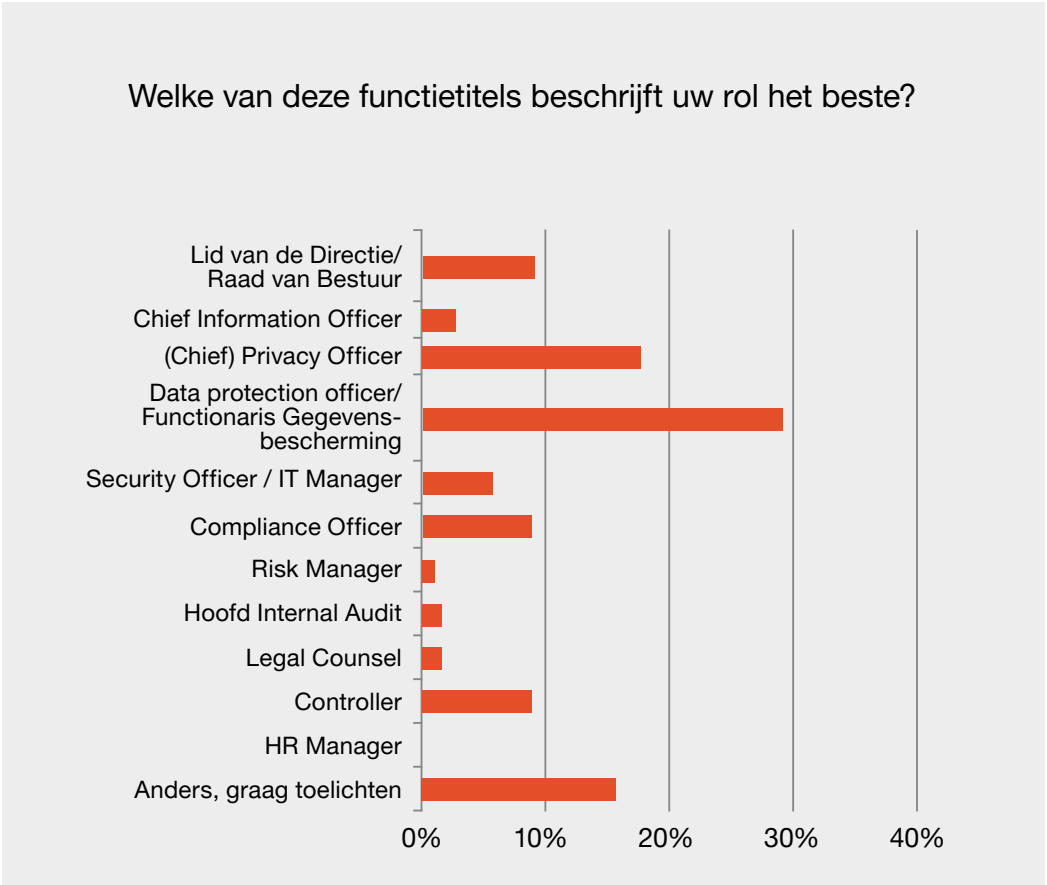
Een kwart van de respondenten geeft aan dat onvoldoende mankracht het grootste struikelblok is voor borging van compliance van de AVG. Slechts **15%** van de organisaties ziet geen struikelblok om blijvend te voldoen aan de AVG.

Wat ziet uw organisatie als de voornaamste struikelblokken om te blijven voldoen aan de privacywetgeving? (Meerdere antwoorden mogelijk)

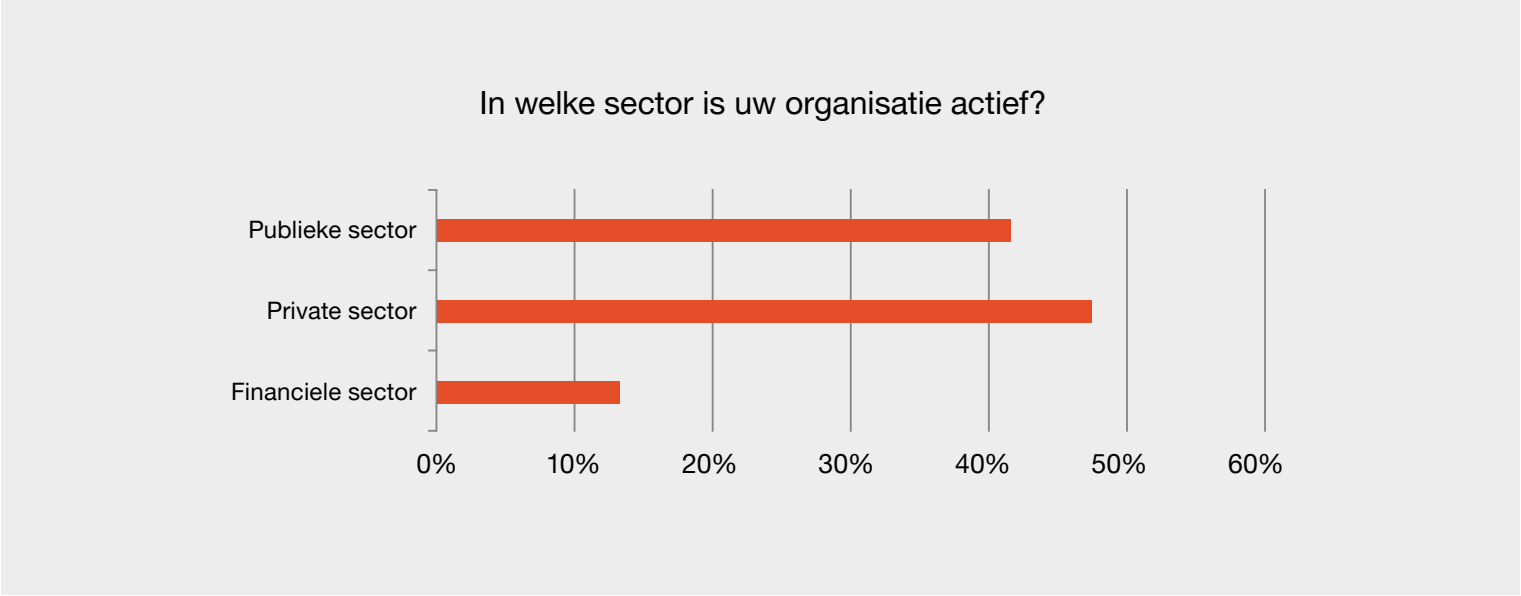


Over u en uw organisatie

De individuele respondenten van de survey zijn werkzaam in een grote verscheidenheid aan functies.



Over u en uw organisatie



Bijlagen

Bijlage A: PwC Privacy Portfolio

Legal services

- Interpretation of the GDPR
- Opinion on extent of legal compliance
- Support before the regulator and the courts
- Drafting, advice etc.

Regulatory liaison

- We have excellent relationships with regulators all over the world
- Former regulators are members of our team

Bench-marking

- International
- Sectoral
- Functional

Consulting services

- Strategy development
- Process development and change
- Technology implementations
- Training and awareness (including e-learning)

Risk advisory and assurance

- Privacy Impact Assessments
- Controls advice and reviews
- Internal audit
- Information Governance
- Cyber Security

Forensics services

- Search and e-Discovery
- Data mapping
- Data classification
- Weeding and de-duplification

We furthermore offer a multi-lingual hosted e-learning suite for GDPR:
For more info refer to link

Contactgegevens

Meer weten over het Privacy Governance onderzoek en wat PwC voor uw organisatie kan doen?
Neem contact op met:

Bram van Tiel
Director Cybersecurity and privacy
+31 (0)88 792 53 88
bram.van.tiel@pwc.com

Yvette van Gemerden
Partner Legal Services
+31 (0) 88 792 54 42
yvette.van.gemerden@pwc.com

© 2019 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.