Privacy Governance onderzoek

Volwassenheid van privacybeheersing binnen Nederlandse organisaties

PwC Nederland

mei 2018

pwc

Inhoudsopgave

Introductie PwC Privacy Governance onderzoek 2018

Vanaf 2014 voert PwC jaarlijks een breed Privacy Governance onderzoek uit. Voor u ligt alweer het vijfde jaarlijkse onderzoeksrapport en het tweede in samenwerking met de NOS. Op het moment dat u dit rapport leest is de overgangstermijn uit de Algemene Verordening Gegevensbescherming (AVG) verstreken en is de AVG volledig van toepassing op alle verwerkingen van persoonsgegevens binnen uw organisatie.

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. In veel gevallen is de verantwoordelijkheid voor het onderwerp op een hoger niveau komen te liggen en er zijn door het hele land talloze data protection officers (DPO) en functionarissen voor gegevensbescherming (FG) opgeleid en benoemd.

Daarnaast zijn kennis van de relevante wet- en regelregelgeving en bewustwording van het belang van privacy over de hele linie toegenomen. Dit betekent niet dat er vanaf dit moment achterover kan worden geleund. Voor veel organisaties geldt dat er nog gaten te vullen zijn. Zo blijkt uit de laatste onderzoeksresultaten dat slechts 42% van de organisaties heeft aangegeven per 25 mei 2018 compliant te zullen zijn.

www.pwc.nl/privacy

Een jaar geleden verwachtte nog meer dan de helft van de organisaties deze deadline te zullen halen. Hieruit komt het beeld naar voren dat het voor organisaties kennelijk moeilijker is dan eerder gedacht om alles te realiseren en dat het besef van de complexiteit van de materie steeds meer begint door te dringen.

Ook de organisaties die aangeven wel al volledig compliant te zijn, kunnen het zich niet veroorloven achterover te gaan leunen. Compliance is een continu proces dat aandacht en betrokkenheid vanuit de gehele organisatie vereist. Dat gaat verder dan de juridische, HR en IT security afdeling. Het creëren en op een pijl houden van bewustwording van het belang van privacy dient door organisaties blijvend te worden ondersteund. Daarbij zijn in vele gevallen veranderingen in ingesleten bedrijfsprocessen en werkwijzen noodzakelijk. De cultuuromslag die daar in veel gevallen voor nodig is, is lang niet altijd eenvoudig te bewerkstelligen en te bestendigen. Alleen al op dat gebied is voor de DPO's, FG's en andere privacy verantwoordelijken de komende jaren nog volop werk aan de winkel.

Tot slot hebben wij in ons onderzoek nadrukkelijker stilgestaan bij het gebruik van technologie om privacy compliant te worden en te blijven, maar ook om meer waarde uit de gedane privacy investeringen te halen. Hieruit blijkt dat slechts 29% van de deelnemende organisaties heeft geïnvesteerd in technologie om compliant met de AVG te worden. Ook als wij nader inzoomen op de afhandelingen van de verschillende rechten van betrokkenen (o.a. inzage, correctie, wissen of overdragen van persoonsgegevens) zien wij dat slechts 16% dit (deels) heeft geautomatiseerd. Ook het vastleggen van toestemming (consent) gebeurd in slechts 26% van gevallen geautomatiseerd. Met andere woorden, op het gebied van technologie en het optimaliseren en automatiseren van processen is nog veel te winnen.

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 regelgeving. Dit onderzoek biedt de mogelijkheid om de staat van de privacy governance in 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 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 is er veranderd op het gebied van privacywetgeving?

De AVG heeft een grote impact op verwerking en bescherming van persoonsgegevens binnen organisaties. Belangrijke veranderingen vanuit de AVG zijn het aantoonbaar maken van inzicht in de verwerkingsprocessen en in de datastromen van persoonsgegevens. Verder moet privacy bij de introductie van nieuwe producten en/of systemen zijn geborgd (privacy by design & privacy by default). Op basis van de AVG ontstaat tevens een fors hogere boetebevoegdheid met boetes die kunnen oplopen tot het hogere van 4% van de wereldwijde jaaromzet of een bedrag van EUR 20.000.000.

Vanwege de zogenaamde extra-territoriale werking van de AVG, krijgen ook organisaties die niet (uitsluitend) in de EU zijn gevestigd met deze strenge privacy wetgeving te maken. Buiten de EU gevestigde organisaties moeten mogelijkerwijs een vertegenwoordiger in de EU aanwijzen die verantwoordelijk en aanspreekbaar is op het gebied van privacy aangelegenheden.

We zien dat bij steeds meer organisaties de voorbereidingen voor de AVG daadwerkelijk op gang zijn gekomen. In 2016 lag de nadruk nog vooral op inventarisatie van de staat van de eigen privacy governance ten opzichte van de AVG (via zogenaamde gap assessments). Omdat de deadline van 25 mei 2018 inmiddels is verstreken is dit steeds meer verschoven naar daadwerkelijke implementatie van noodzakelijk beleid en relevante bedrijfsprocessen en procedures. Tevens zal er nu begonnen moeten worden om na te gaan hoe organisaties aantoonbaar gaan maken en gaan borgen dat ze op continue wijze voldoen aan de vereisten die voortvloeien uit de AVG.

Uitsplitsing van de resultaten

De afgelopen jaren hebben inmiddels ruim 900 organisaties, uit verschillende sectoren en regio's, deelgenomen aan het PwC Privacy Governance onderzoek, waarvan 385 organisaties dit jaar. De resultaten zijn na de managementsamenvatting 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 voor te bereiden op de aanstaande regelgeving uit de AVG.
2. De openstaande punten op basis van risico's en prioriteitsstelling te vertalen naar een concreet actieplan dat onder meer moet leiden tot het doorvoeren van organisatorische, procedurele en technische verbeteringen.
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. Bovendien verschaft het rapport 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
Yvette van Gemerden
Adri de Bruijn

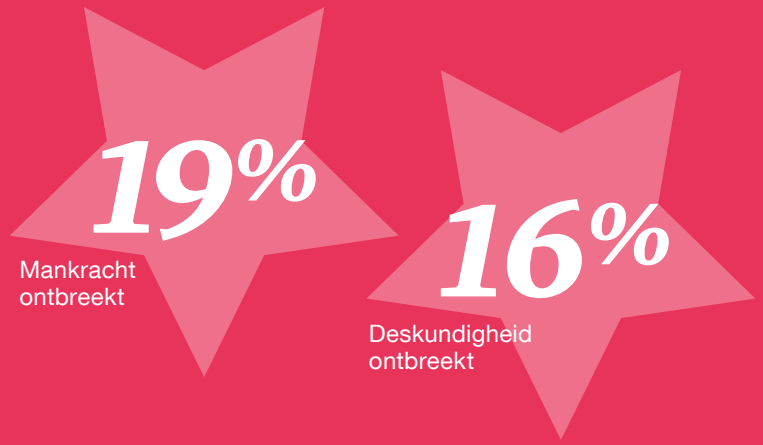
Managementsamenvatting

Merendeel organisaties niet tijdig compliant

Slechts ***42%*** van de deelnemende organisaties zegt op 25 mei 2018 compliant te zijn (vorig jaar verwachtte nog ***52%*** tijdig klaar te zijn).

Zorgen over borging van privacy

Het ontbreken van voldoende mankracht (***19%***) en deskundigheid (***16%***) worden door organisaties als grootste risico's genoemd voor het borgen van privacy in de toekomst.



Overzicht van verwerkingen van persoonsgegevens is beperkt aanwezig

Het aantal organisaties dat een volledig overzicht van verwerkingen heeft is zeer beperkt. Slechts ***19%*** van de respondenten heeft een dergelijk verwerkingsregister en ***39%*** van de organisaties zegt er nog mee bezig te zijn. Het hebben van een register van verwerkingen is essentieel voor het verdere proces naar compliance met de AVG.

Privacy budgetten blijven op hetzelfde niveau

De groei van privacybudgetten stagneert. Nog slechts ***22%*** van de deelnemende organisaties geeft aan dat er sprake is geweest van een toename van het budget ten opzicht van het voorgaande jaar.

Bijna een derde van de organisaties investeert in technologie

29% van de deelnemende organisaties heeft gedurende de afgelopen 12 maanden investeringen gedaan op technologisch gebied met het oog op AVG compliance.

29%

Procedures of richtlijnen voor rechten van betrokkenen worden geïmplementeerd

Steeds meer organisaties ***(45%)*** hebben procedures ingericht om verzoeken van betrokkenen (o.a. inzage, correctie, wissen of overdragen van persoonsgegevens) af te handelen. Hierbij wordt slecht in ***16%*** van gevallen gebruik gemaakt van technologie.

Klein deel van de organisaties heeft een privacy officer aangesteld

16% van de deelnemers heeft de verantwoordelijkheid voor privacy belegd bij de privacy officer. Aan de andere kant zijn er nog steeds relatief veel ***(23%)*** organisaties die het onderwerp privacy nergens hebben belegd.

Risico op niet naleven wettelijke bewaartermijnen is groot bij veel organisaties

Organisaties worstelen nog altijd met naleving van bewaartermijnen. Een derde van de organisaties geeft aan geen bewaartermijnenbeleid te hebben geïmplementeerd.

Data Protection Impact Assessments (DPIAs) worden door weinig organisaties uitgevoerd

De helft van de organisaties voert nog altijd geen risicoanalyses uit (DPIA's) in het kader van omgang met persoonsgegevens.

50%

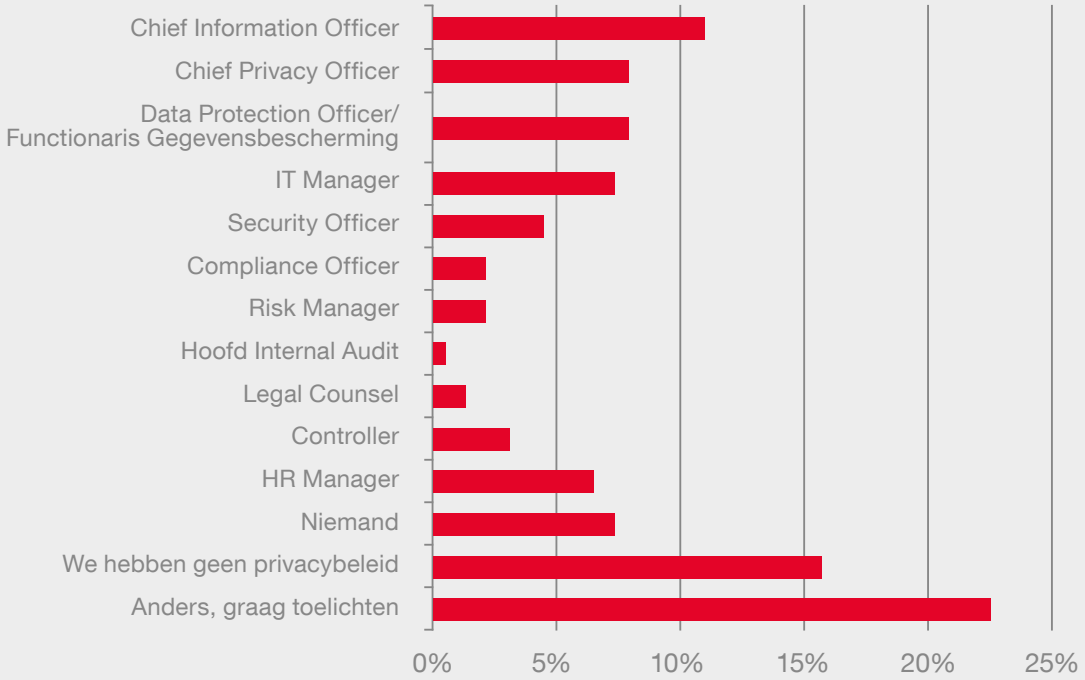
Resultaten

Privacy Strategie en Beleid

Organisaties beleggen de verantwoordelijkheid voor het onderwerp privacy bij verschillende rollen. Hierbij zien wij dat de benoeming van een Privacy Officer (of Functionaris voor de Gegevensbescherming) stagneert, want met ***16%*** organisaties die een dergelijke functie heeft belegd is dit nagenoeg gelijk gebleven met vorig jaar.

In ***23%*** van de gevallen is de verantwoordelijkheid voor het privacybeleid niet belegd of is er in het geheel geen sprake van een privacybeleid.

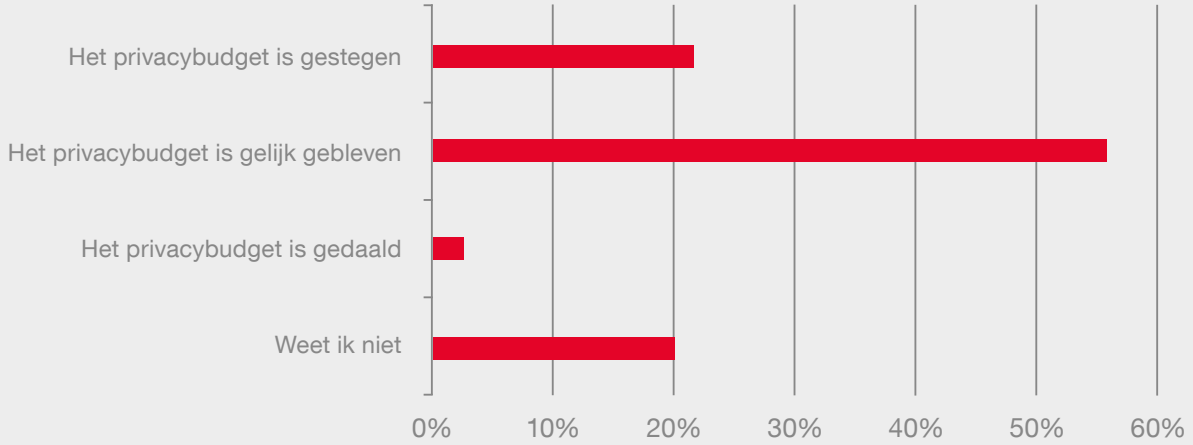
Wie is er op dit moment binnen uw organisatie primair verantwoordelijk voor het privacybeleid?



Privacy Strategie en Beleid

Bij slechts **22%** van de organisaties zijn gedurende het afgelopen jaar extra investeringen gedaan op het gebied van privacy compliance en governance.

Wat is de ontwikkeling van het privacybudget in vergelijking met 2017?

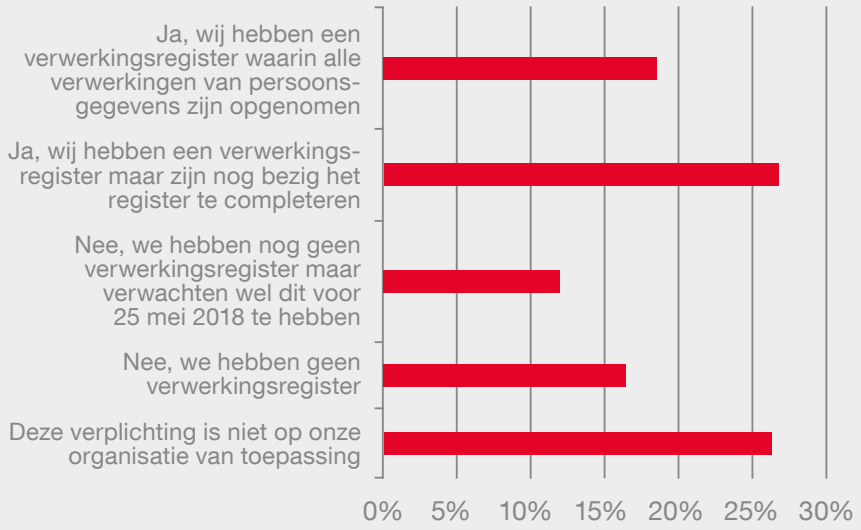


Privacy Strategie en Beleid

De Europese Privacy Verordening legt organisaties op om een gedetailleerde beschrijving van de verwerkingen van persoonsgegevens op te stellen en bij te houden.

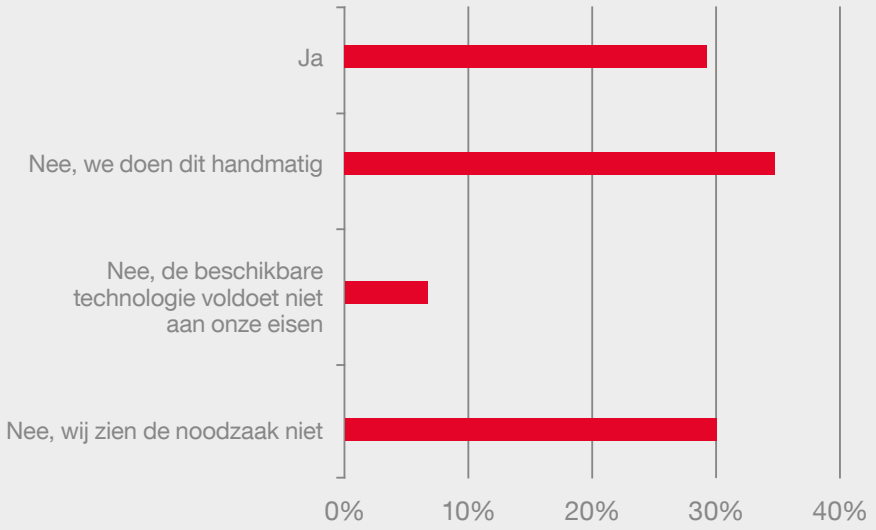
Slechts ***19%*** van de organisaties voldoet al aan de verplichting uit de AVG om alle verwerkingen van persoonsgegevens inzichtelijk te hebben en te documenteren. Bij een ruime meerderheid zijn verwerkingen van persoonsgegevens niet of nauwelijks gedocumenteerd.

Houdt uw organisatie een register van verwerkingsactiviteiten bij?



Slechts ***29%*** van de deelnemende organisaties heeft geïnvesteerd in technologie om compliant met de AVG te worden en blijven. ***30%*** ziet op dit moment geen noodzaak om technologie te gebruiken om aantoonbaar te maken dat de organisatie voldoet aan de AVG.

Heeft uw organisatie geïnvesteerd in technologie om compliant met de Algemene Verordening Gegevensbescherming te worden?



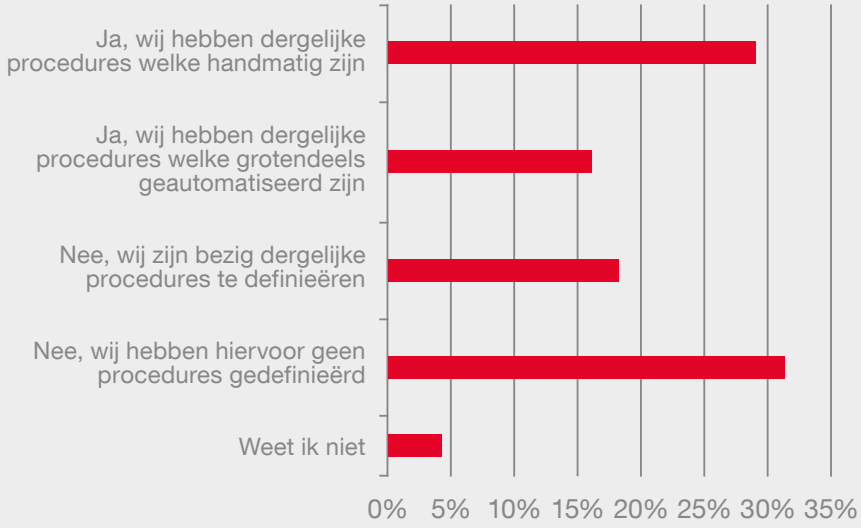
Privacy Strategie en Beleid

De helft van de organisaties heeft nog geen enkele procedure geïmplementeerd voor de afhandeling van inzage- en correctieverzoeken, overdracht van gegevens of verzoeken om vergeten te worden van betrokkenen. Slechts ***16%*** van de organisatie heeft (delen) van deze processen geautomatiseerd, voor de meeste organisatie geldt dan ook dat het voldoen aan dergelijke verzoeken een handmatig proces is.

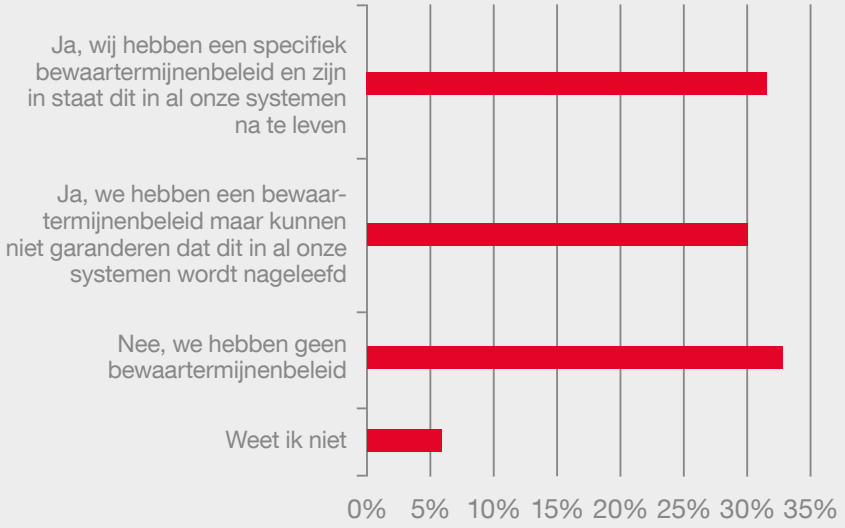
Beleid op het gebied van bewaartermijnen en de verwijdering van persoonsgegevens is door ***61%*** van de deelnemende organisaties vastgesteld.

Slecht ***31%*** van organisatie geeft aan dat het bewaartermijnenbeleid ook wordt nageleefd.

Heeft uw organisatie procedures om verzoeken van betrokkenen af te handelen, zoals verzoeken om inzage, correctie, overdracht of het wissen van persoonsgegevens?



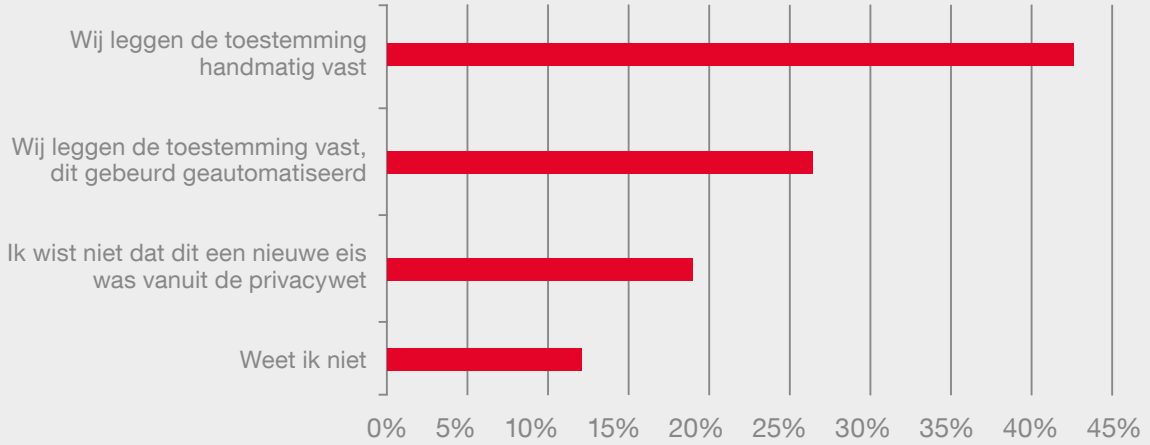
Worden binnen uw organisatie alle wettelijke bewaartermijnen voor persoonsgegevens adequaat nageleefd?



Privacy Strategie en Beleid

69% van de organisaties legt de toestemming van betrokkene inzake verwerking van hun persoonsgegevens vast, ook hier gebruikt slechts een klein deel (***26%***) technologie om dit geautomatiseerd te doen.

Legt uw organisatie de toestemming van betrokkene inzake verwerking van hun persoonsgegevens vast?

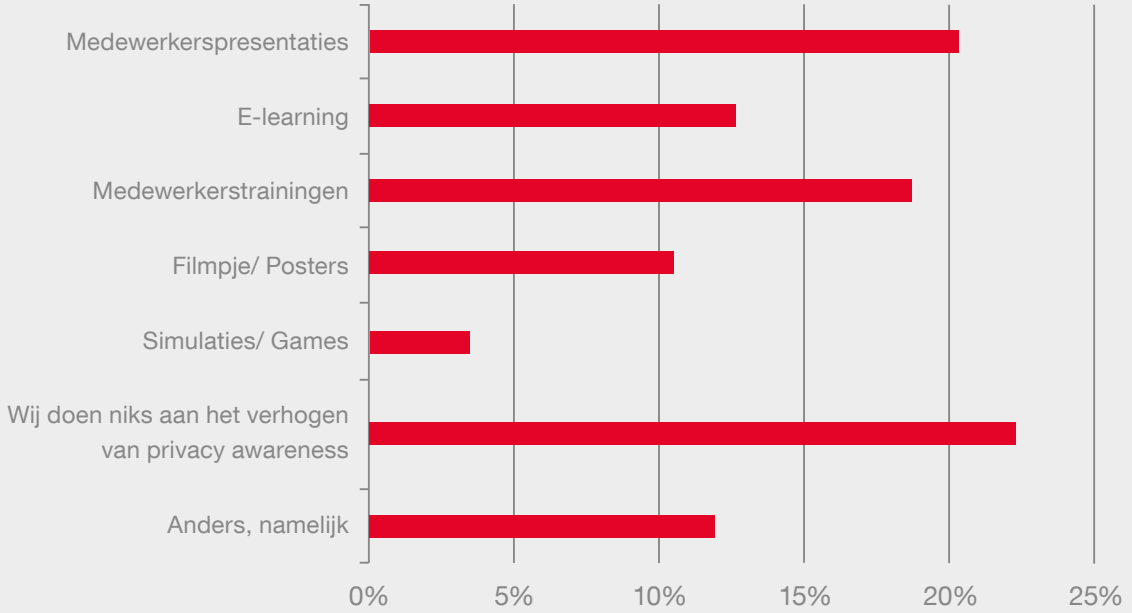


Privacy Strategie en Beleid

Ruim een vijfde (**22%**) van de organisaties doet op dit moment nog niets aan het verhogen van de privacy awareness.

De organisaties die wel wat aan awareness doen, houden in **20%** van de gevallen medewerkerspresentaties, veelal gecombineerd met trainingen.

Hoe heeft u de privacy awareness binnen uw organisatie verhoogd?



Privacy incidenten en meldingen

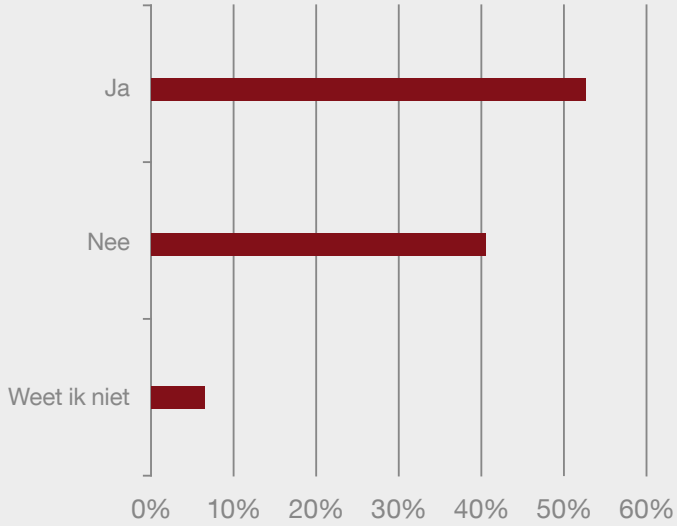
Vanaf 1 januari 2016 bestaat voor alle organisaties de verplichting om datalekken onverwijld te melden bij de Autoriteit Persoonsgegevens (AP) en in bepaalde gevallen ook betrokkenen hierover te informeren. Bij de melding moeten onder meer de impact van het datalek en de ter zake te nemen maatregelen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

Met ***34%*** geeft een ruime minderheid van de deelnemers aan dat de eigen organisatie goed tot zeer goed heeft gereageerd op privacy incidenten die zich hebben voorgedaan. Dit is lager dan voorgaande jaren.

Ruim de helft (***53%***) van de organisaties geeft aan te voldoen aan de verplichting om een overzicht van datalekken bij te houden.

Hoe reageert uw organisatie naar uw oordeel op de privacy incidenten (bijvoorbeeld datalekken) die zich in de organisatie voordoen?

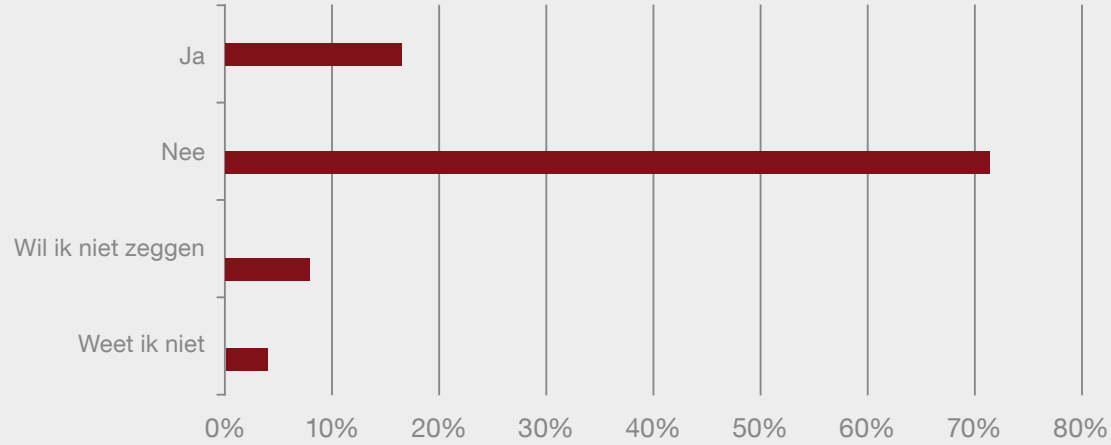
Houdt uw organisatie een overzicht bij van datalekken?



Privacy incidenten en meldingen

Bij ***17%*** van de organisaties hebben zich het afgelopen jaar één of meerdere datalekken voorgedaan die zijn gemeld bij de Autoriteit Persoonsgegevens.

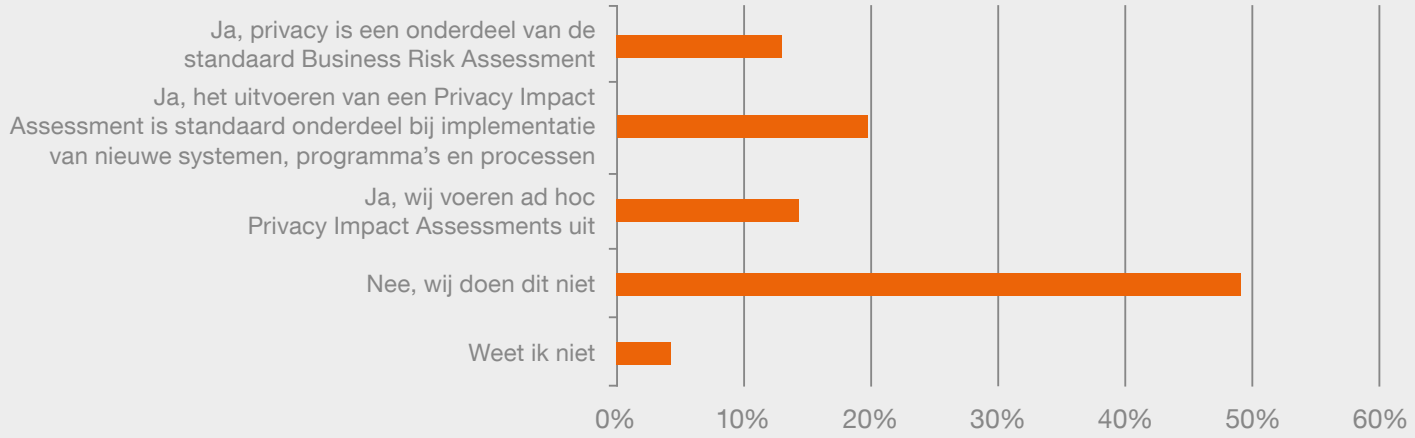
Heeft uw organisatie het afgelopen jaar een datalek gemeld bij de Autoriteit Persoonsgegevens?



Uw organisatie en het privacyrisico

Slechts ***33%*** van de organisaties voert met regelmaat risicoanalyses (zoals Data Protection Impact Assessments) uit. ***14%*** doet dit uitsluitend op ad hoc basis terwijl ***53%*** van de deelnemende organisaties aangeeft helemaal geen risicoanalyses uit te voeren, of dit niet weet in het kader van de omgang met persoonsgegevens.

Voert uw organisatie risicoanalyses uit (bijvoorbeeld Data Protectie Impact Assessments) in het kader van omgang met persoonsgegevens?



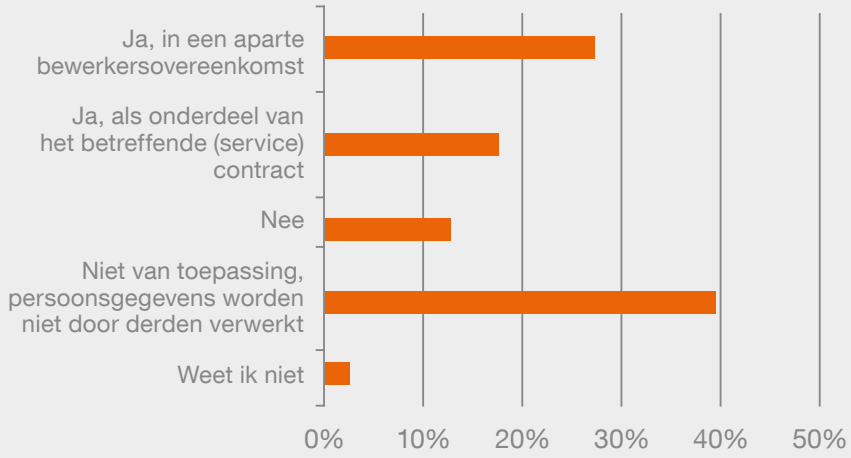
Uw organisatie en het privacyrisico

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.

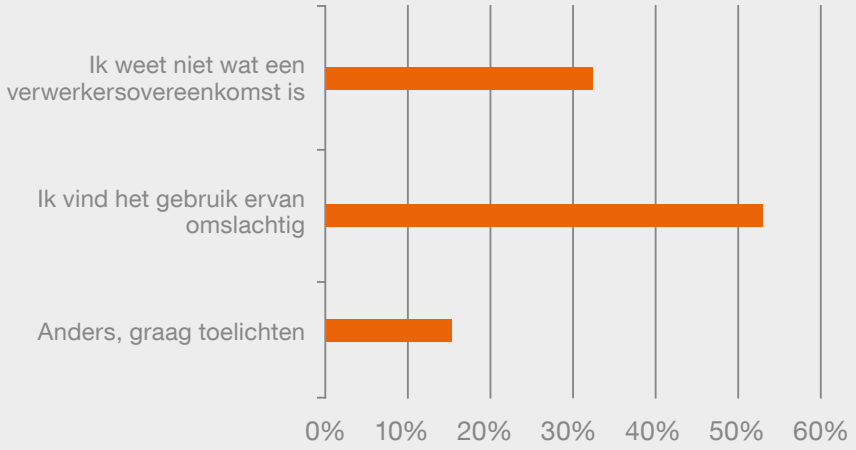
Door ***ongeveer 45%*** van de organisaties worden contractuele verplichtingen met verwerkers van persoonsgegevens vastgelegd in aparte verwerkersovereenkomsten of als onderdeel van het servicecontract. Slechts ***13%*** van de organisaties legt contractuele verplichtingen inzake omgang met persoonsgegevens nog helemaal niet vast.

Ruim de helft (***53%***) van de organisaties die geen gebruik maken van verwerkersovereenkomsten doen dat omdat ze dit te omslachtig vinden. Een ***derde*** (***31%***) weet niet wat een verwerkersovereenkomst is.

Maakt u gebruik van verwerkersovereenkomsten indien u persoonsgegevens door derden laat bewerken?



Waarom maakt u geen gebruik van verwerkersovereenkomsten?

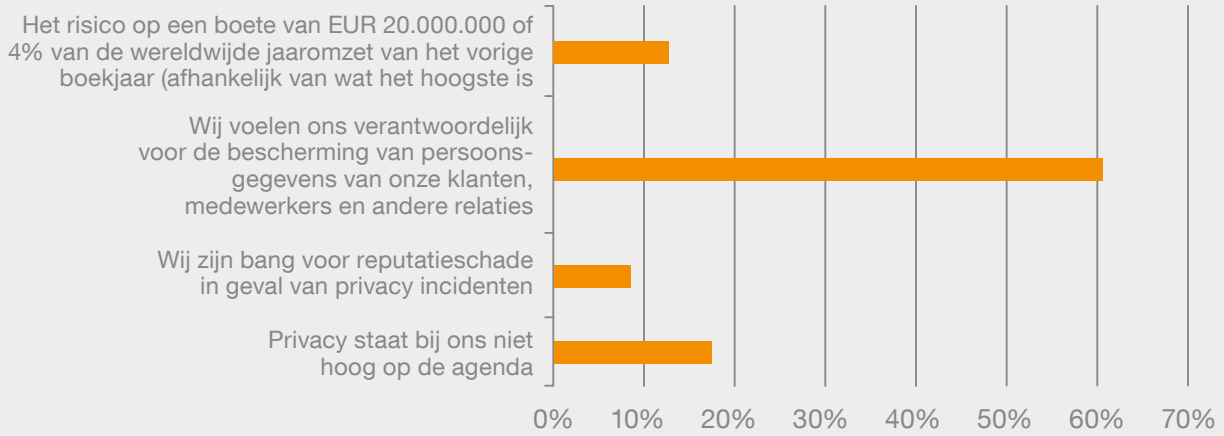


Stellingen

Een ruime meerderheid ***(61%)*** van de organisaties geeft als belangrijkste reden om privacy hoog op de agenda te zetten aan, zich verantwoordelijk te voelen voor de bescherming van persoonsgegevens van klanten, medewerkers en andere relaties.

Bij slechts een gering aantal organisaties ***(13%)*** is het onder de aanstaande AVG versterkte boeteregime daarvoor de belangrijkste reden.

De belangrijkste reden voor onze organisatie om privacy hoog op de agenda te zetten is:

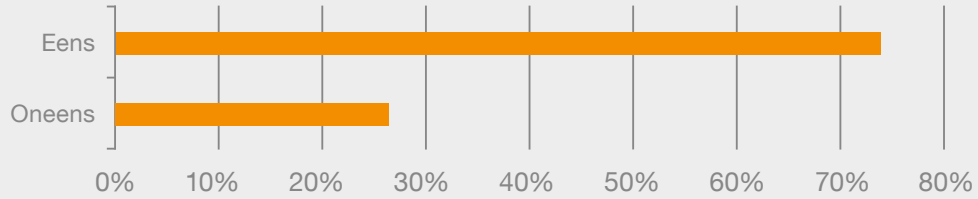


Stellingen

Op basis van de AVG wordt het 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 nieuwe verplichting geeft ***26%*** van de deelnemende organisaties aan bij de ontwikkeling van nieuwe systemen nog niet altijd rekening mee te houden.

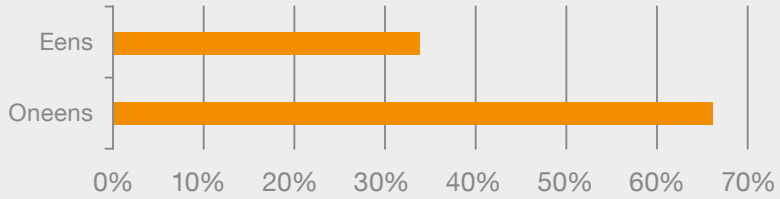
Bij implementatie van nieuwe systemen houden wij altijd in een vroeg stadium rekening met privacy aspecten en de bescherming van persoonsgegevens (Privacy by Design & Privacy by Default principes):



Stellingen

Twee derde (66%) van de respondenten ervaart privacyregelgeving niet als belemmerend voor de innovatie-mogelijkheden van de organisatie.

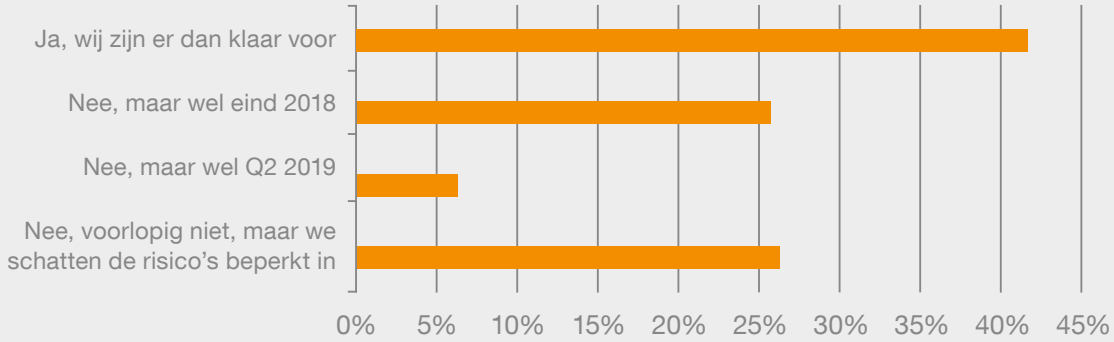
Privacyregelgeving beperkt onze innovatiemogelijkheden:



Stellingen

Slechts ***42%*** van de organisaties verwacht op 25 mei 2018 klaar te zijn voor de AVG, ***26%*** van de organisaties verwacht gereed te zijn met de implementatie van de maatregelen voor de AVG eind 2018. ***33%*** van de organisaties geeft aan voorlopig niet klaar te zijn, maar schatten de risico's in als beperkt

Wij zijn per 25 mei 2018 klaar voor de wijzigingen in de privacyregelgeving (Algemene Verordening Gegevensbescherming):

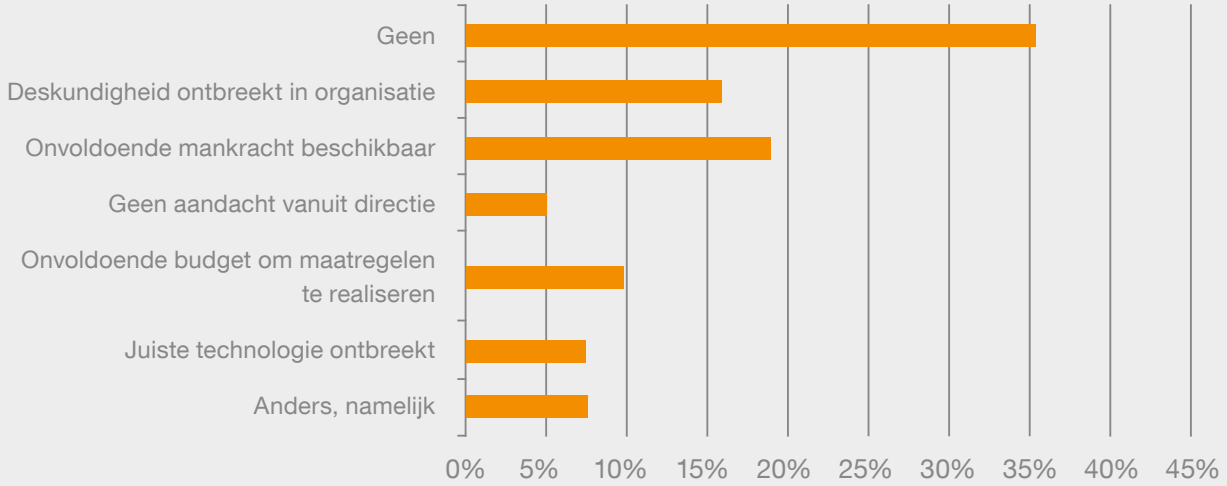


Stellingen

19% van de respondenten geeft aan dat onvoldoende mankracht het grootste struikelblok is voor borging van compliance na 25 mei 2018. ***16%*** geeft aan dat de deskundigheid ontbreekt in de organisatie.

Ruim ***een derde*** van de organisaties ziet geen struikelblok om na 25 mei 2018 blijvend te voldoen aan de AVG.

Wat ziet u voor uw organisatie als het grootste struikelblok voor de borging van de Algemene Verordening Gegevensbescherming na 25 mei 2018?

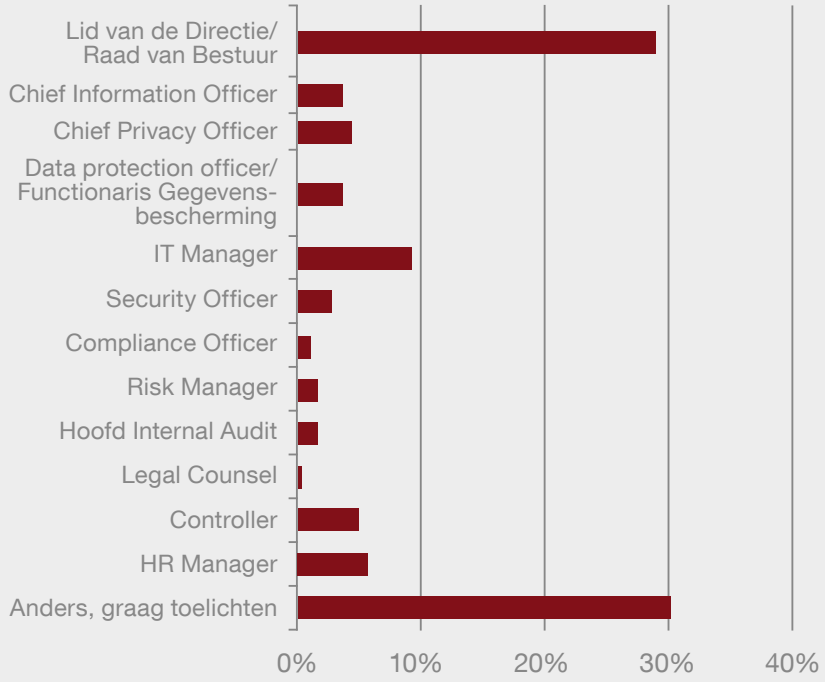


Over u en uw organisatie

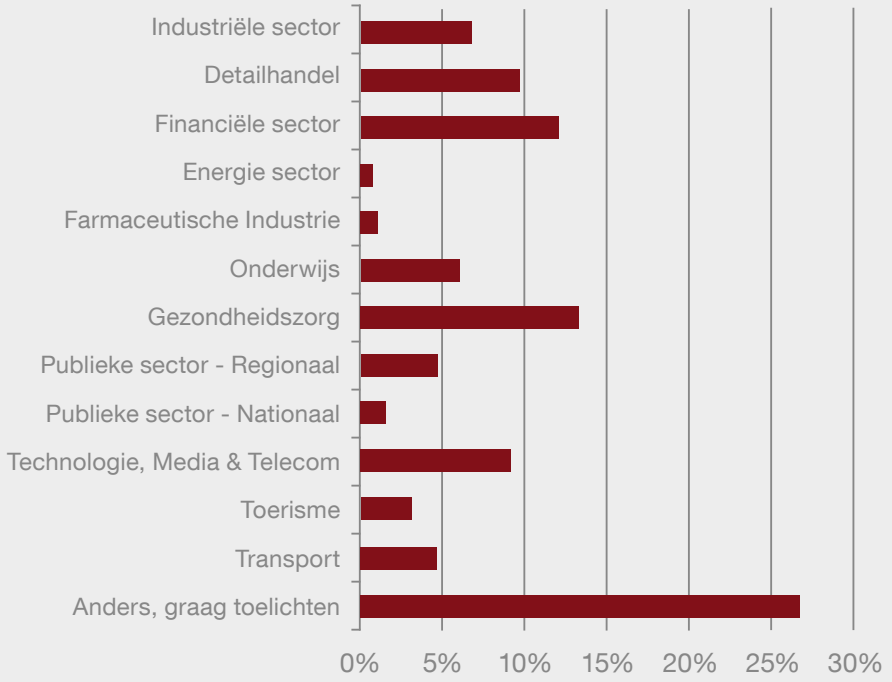
De individuele respondenten van de survey zijn werkzaam in een grote verscheidenheid aan functies.

De deelnemende organisaties zijn actief in een grote verscheidenheid aan sectoren.

Welke van deze functietitels beschrijft uw rol het beste?



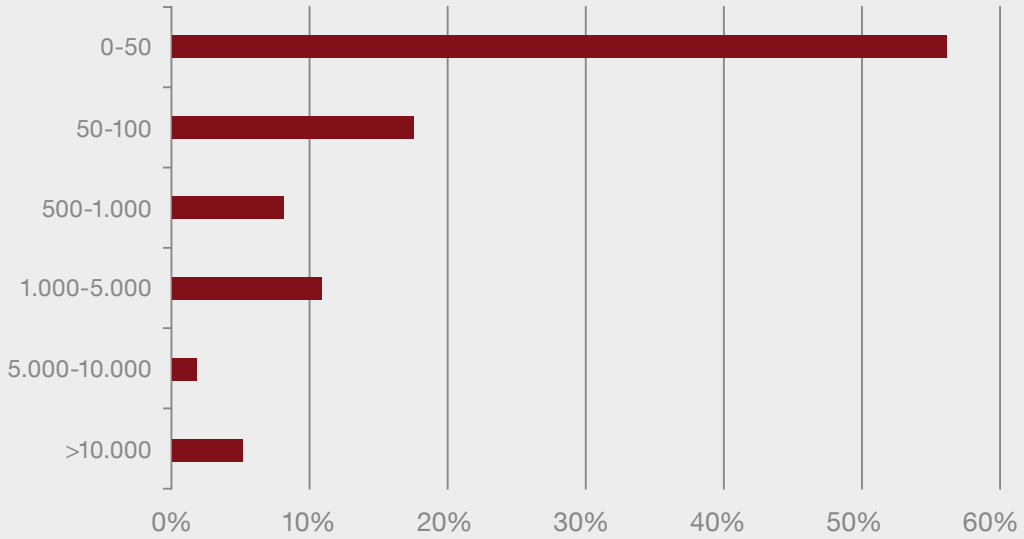
Welke sectorclassificering is het meest van toepassing op de belangrijkste activiteiten van uw organisatie?



Over u en uw organisatie

74% van de deelnemende organisaties heeft minder dan 500 werknemers, ***13%*** van de organisaties heeft tussen de 1.000 en 5.000 werknemers en ***5%*** heeft meer dan 10.000 werknemers.

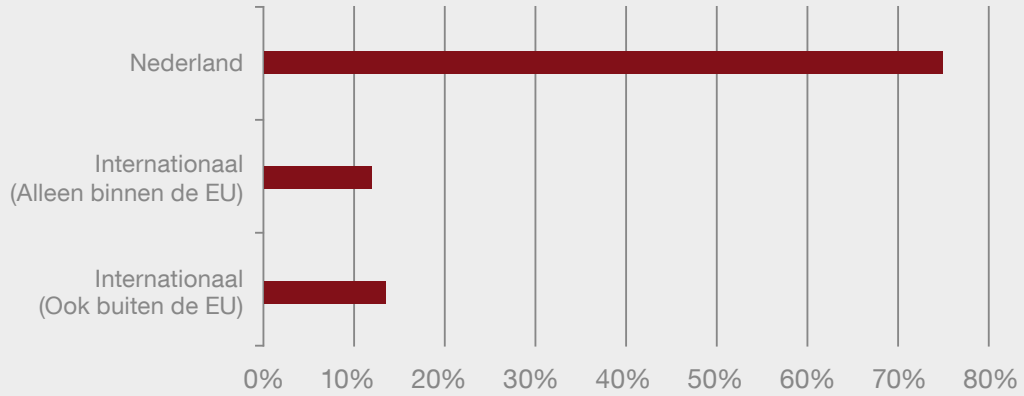
Hoeveel werknemers heeft uw organisatie wereldwijd?



Over u en uw organisatie

Bij ***75%*** van de deelnemende organisaties zijn de activiteiten voornamelijk op Nederland gericht.

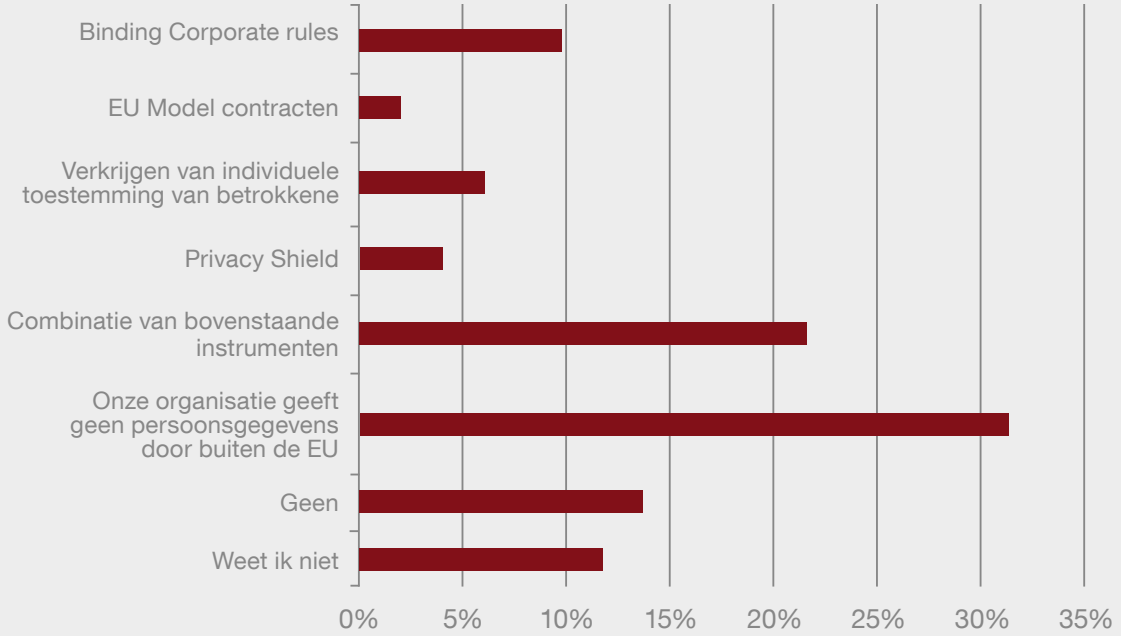
Richt uw organisatie haar activiteiten voornamelijk op Nederland, de EU, of Internationaal?



Over u en uw organisatie

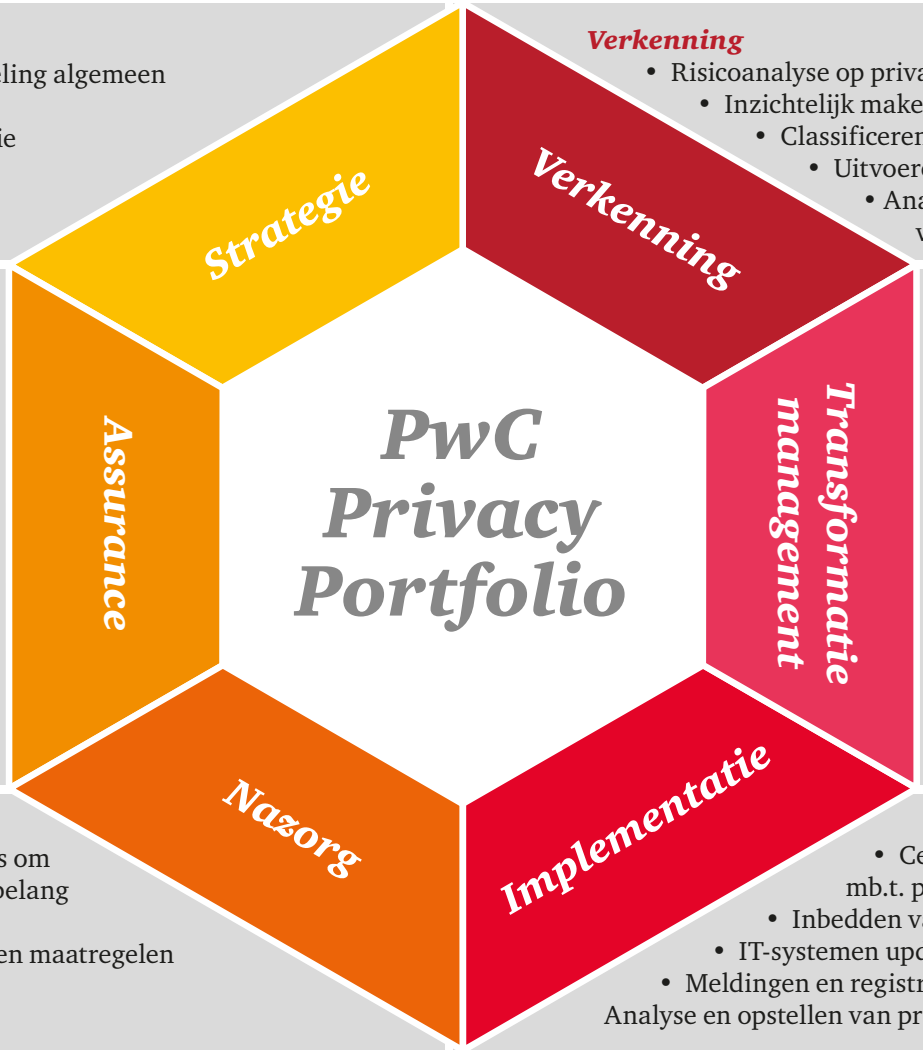
In geval van het versturen van persoonsgegevens naar buiten de EU maakt ***14%*** van de organisaties (nog) geen gebruik van één van de daarvoor noodzakelijke instrumenten.

Welke van onderstaande instrumenten heeft uw organisatie geïmplementeerd voor het beheren van persoonsgegevens die buiten de EU verstuurd worden?



Bijlagen

Bijlage A: Hoe kan PwC u helpen?



Strategie
- Ondersteunen bij ontwikkeling algemeen privacy beleid
- Vormgeven privacy strategie
- Opstellen privacy roadmap
- Verhogen van het privacy bewustzijn

Verkenning
- Risicoanalyse op privacy gevoelige gegevens
- Inzichtelijk maken van de mogelijkheden voor gebruik van persoonsgegevens
- Classificeren van de privacy gevoelige data
- Uitvoeren van een nulmeting
- Analyse van contractuele structuren rondom de verwerking van persoonsgegevens

Assurance
- Afgeven van Assurance rapporten o.b.v. Standaard 3000A/ SOC2
- Afgeven van privacy certificering

Transformatie Management
- Ondersteunen AVG transformatieprojecten
- Opstellen van een privacy programma
- Inzichtelijk maken van benodigde veranderingen in IT-systemen
- Uitvoeren GAP-analyses
- Uitvoeren Privacy Impact Assessment
- Uitvoeren Contract assessments

Nazorg
- Organiseren van workshops om medewerkers te wijzen op belang van privacy
- Privacybeleid en de genomen maatregelen publiceren op Intranet
- Governance beoordelingen

Implementatie
- Centraal beleggen van verantwoordelijkheden mb.t. persoonsgegevens
- Inbedden van privacy maatregelen in het huidige controle raamwerk
- IT-systemen updaten om maatregelen systeemtechnisch af te dwingen
- Meldingen en registraties bij Autoriteit Persoonsgegevens

Analyse en opstellen van privacy policies

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

Adri de Bruijn
Partner Consulting Technology
+31 (0) 88 792 65 87
adri.de.bruijn@pwc.com

www.pwc.nl/privacy