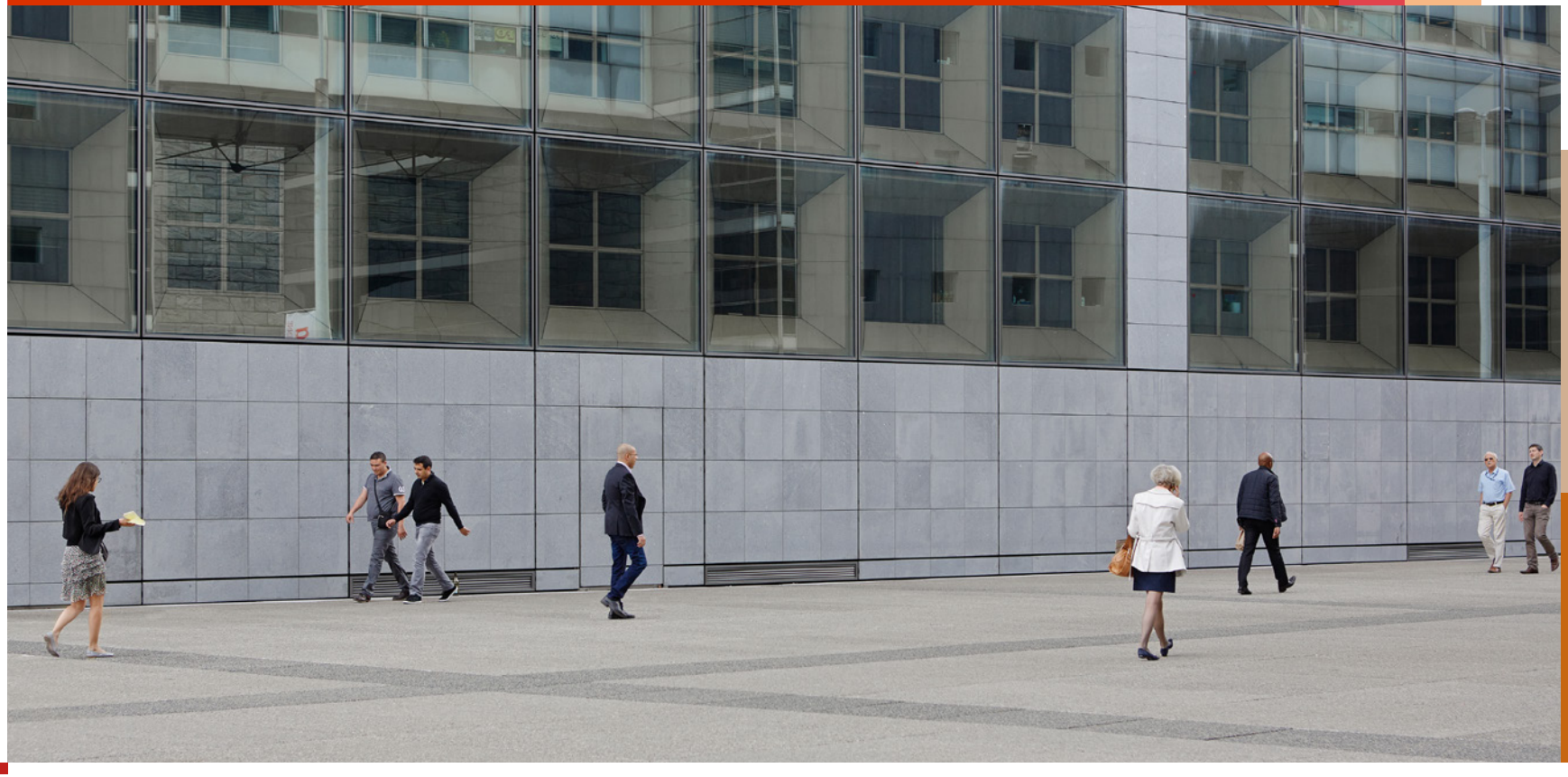
Privacy Governance onderzoek

Volwassenheid van privacybeheersing binnen Nederlandse organisaties



PwC Nederland

januari 2016

pwc

Inhoudsopgave

Introductie PwC Privacy Governance onderzoek

Als vervolg op het succesvolle onderzoek van vorig jaar heeft PwC ook in 2015 weer het Privacy Governance onderzoek uitgevoerd. Het onderwerp privacy stond in 2015 volop in de schijnwerpers! Een greep uit de belangrijkste gebeurtenissen:

- ***De Nederlandse privacy wetgeving is aangescherpt (Meldplicht datalekken);***
- ***Safe Harbor is ongeldig verklaard; en***
- ***De Algemene Verordening Gegevensbescherming (AVG) uit Europa is op de valreep definitief vastgesteld.***

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, wat ze er aan doen en op welke wijze ze omgaan met bestaande en nieuwe regelgeving. Het biedt daardoor de mogelijkheid om uw eigen organisatie te vergelijken met andere organisaties, zonder dat het een oordeel geeft over de privacy prestaties en compliance van uw organisatie als zodanig.

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

Het Privacy Governance onderzoek verschaft een uniek beeld in hoeverre uw organisatie klaar is voor de nieuwe Algemene Verordening Gegevensbescherming (AVG) en in de mate van volwassenheid inzake de bescherming van persoonsgegevens. Daarnaast biedt het de mogelijkheid om de resultaten te vergelijken met andere voor u relevante organisaties. De publicatie geeft daarmee een eerste inzicht in de wijze waarop organisaties in Nederland omgaan met het onderwerp privacy.

Toegevoegde waarde voor u en uw organisatie zijn de volgende:

- beter begrip van de aard en impact van nieuwe privacywetgeving;
- balans opmaken van de voor u relevante privacyrisico's;
- evaluatie van privacy governance en resilience in uw eigen organisatie.

www.pwc.nl/privacy

Welke nieuwe eisen stelt de wetgeving?

Een belangrijke wetswijziging waarmee alle organisaties die persoonsgegevens verwerken met ingang van 1 januari 2016 te maken hebben gekregen is de aanscherping van de Wet bescherming persoonsgegevens (Wbp), ook wel de Meldplicht Datalekken genoemd. Hierin is de verplichting tot het melden en beheersen van een datalek vastgelegd. Tevens geeft het de toezichthouder (Autoriteit Persoonsgegevens) de mogelijkheid tot het uitdelen van hoge boetes (tot € 820.0000).

Daarnaast krijgen organisaties binnen de EU te maken met de bindende regels uit de AVG. Naar verwachting treedt de AVG in het voorjaar van 2016 officieel in werking en krijgen organisaties 2 jaar de tijd om aan deze nieuwe regels te voldoen. Het is duidelijk dat de AVG grote impact krijgt op beleid en uitvoering rondom bescherming van persoonsgegevens binnen organisaties. Ook op basis van de AVG ontstaat een fors hogere boetebevoegdheid met boetes die kunnen oplopen tot 4% van de wereldwijde jaaromzet, of EUR 20.000.000. Om compliant te worden aan de nieuwe regelgeving, dienen de organisaties onder meer:

- continu in control te zijn van de verwerkingen van persoonsgegevens (ook wanneer u een beroep doet op bewerkers);
- een compliance dossier aan te leggen (verwerkingen, governancestructuur en verantwoordelijkheid);
- voor de meeste organisaties een privacy officer aan te stellen;
- privacy impact assessments (PIA) uit te voeren en privacy by design/ default principes toe te passen;
- rekening te houden met de nieuwe regelgeving in verband met datalekken;
- meer informatie te verschaffen aan personen van wie de organisatie gegevens verwerkt.

Uitsplitsing van de resultaten

De afgelopen 2 jaar hebben 156 organisaties, uit verschillende sectoren, deelgenomen aan het PwC Privacy Governance onderzoek. De resultaten van dit jaar zijn grafisch weergegeven in de volgende hoofdstukken:

- Privacy in uw organisatie
- Privacy Strategie en Beleid
- Privacy incidenten en meldingen
- Privacy en uw leveranciers
- 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. Het rapport en de aanbevelingen te bespreken met de privacyverantwoordelijken binnen uw organisatie om hen in staat te stellen de strategische richting uit te stippelen.
2. De strategische richting te vertalen in een actieplan dat onder meer moet leiden tot organisatorische, procedurele en technische maatregelen.
3. Periodiek de effectiviteit van deze maatregelen te meten.

Wij geloven dat dit onderzoek de Nederlandse privacy competenties kan versterken en onze gezamenlijke internationale concurrentie- en vertrouwenspositie kan verbeteren. Bovendien geeft dit rapport u een beeld van de benadering van privacy aansturing binnen een groot aantal organisaties en stelt het u in staat om een vergelijking te maken met uw eigen organisatie. De rapportage maakt inzichtelijk hoe de omgang met persoonsgegevens binnen uw organisatie zich verhoudt tot vergelijkbare organisaties en concurrenten. De informatie verkregen via deze survey is uitsluitend gebruikt voor totstandkoming van dit rapport.

Wij zijn uiteraard bereid om de impact van de rapportage nader met u te bespreken, dan wel u te faciliteren bij de ontwikkeling van een actieplan dat past bij uw organisatie en aandachtsgebieden.

Met vriendelijke groet,

Bram van Tiel
Director Technology and Security

Yvette van Gemerden
Partner Legal Services

Adri de Bruijn
Partner Consulting Technology

http://www.pwc.nl/privacy

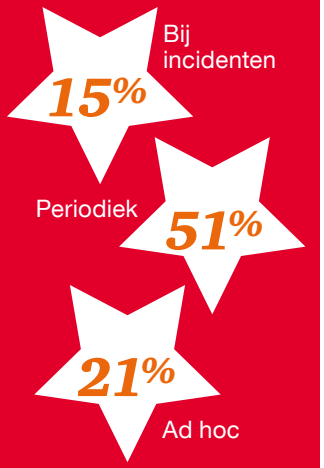
Management Samenvatting

Innovatie niet beperkt door privacy regelgeving

75% van de organisaties voelt zich niet beperkt in zijn innovatiekracht door privacy regelgeving

Samenwerking neemt toe

Het merendeel van de organisaties geeft aan dat privacy een samenspel is tussen Business, Legal en IT (security). Ten opzichte van 2014 is de onderlinge samenwerking substantieel geïntensiveerd



Extra investeringen in privacy compliance

Meer dan ***50%*** van de deelnemers geeft aan het afgelopen jaar extra geïnvesteerd te hebben in privacy compliance

Organisaties nog niet klaar voor meldplicht datalekken

Slechts ***16%*** van de organisaties geeft aan goed of zeer goed voorbereid te zijn op de nieuwe verplichtingen uit hoofde van de Wet meldplicht datalekken. ***11%*** van de respondenten is zelfs nog niet bekend met deze verplichtingen

Minder dan ***de helft*** van de organisaties voldoet aan de wettelijke verplichting om een centraal overzicht van data lekken bij te houden. Maar liefst ***60%*** heeft geen communicatieplan gereed voor het geval er zich een datalek voordoet

Gevolgen ongeldigheid safe harbor nog niet in beeld

Van de organisatie die persoonsgegevens doorgeven naar de VS, geeft bijna de helft aan dat de eigen organisatie nog niet heeft geanalyseerd wat de gevolgen zullen zijn van de ongeldigverklaring van het Safe Harbor verdrag

Gering inzicht in data-stromen en verwerkingen

68% van de organisaties geeft aan ondanks haar verantwoordelijkheid, niet of slechts redelijk zicht te hebben op datastromen naar externe partijen.

13% van de organisaties documenteert alle verwerkingen van persoonsgegevens

Beperkt gebruik en controle bewerkers-overeenkomsten

60% geeft aan gebruik te maken van bewerkers-overeenkomsten bij inzet van leveranciers.

18% controleert op naleving van de bewerkers-overeenkomst

Begrip van de risico's en impact

48% van de deel-nemende organisaties voert geen risico analyses (bijvoorbeeld Privacy Impact Assessments) uit in het kader van omgaan met persoonsgegevens

Organisaties bereiden zich voor op de EU verordening

5% van de deelnemers is klaar voor de verwachte privacyregelgeving. 60% van de organisaties is er zich actief op aan het voorbereiden

60%
In voorbereiding

35%
Niet gestart met voorbereiding

Privacy by design nog niet goed ingebed

Privacy by Design is nog niet goed ingebed binnen organisaties. Ruim ***40%*** houdt geen rekening met gebruik van persoonsgegevens bij introductie van nieuwe systemen

Verschillen in privacy benadering

83% van de deelnemers heeft de verantwoordelijkheid voor privacy expliciet belegd, echter we zien een grote verscheidenheid aan rollen

Resultaten

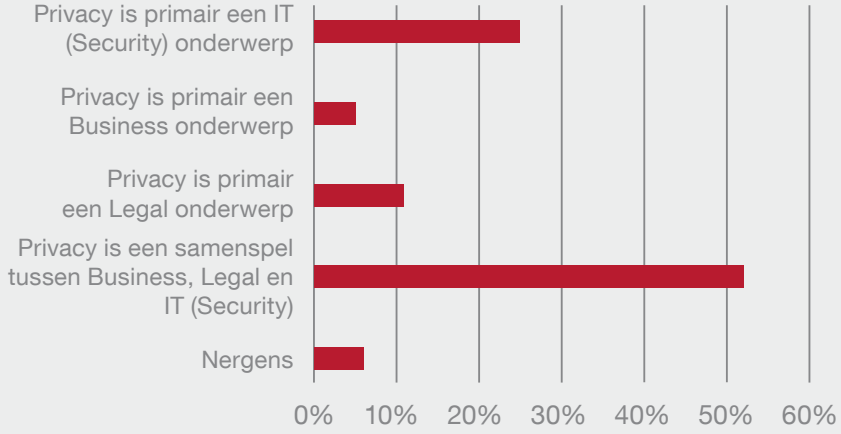
Privacy in uw organisatie

Bij slechts ***52%*** van de organisaties is het onderwerp privacy belegd als een samenspel tussen Business, Legal en IT (Security).

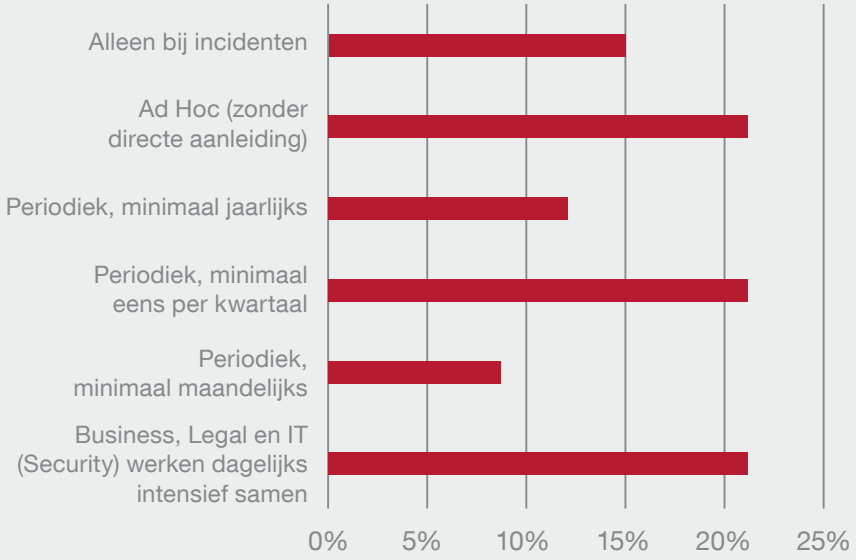
Intensieve samenwerking (via minimaal één keer per kwartaal een bijeenkomst tussen Business, Legal en IT (Security) vindt bij ***51%*** van de organisaties plaats.

Bij ***36%*** van de deelnemers wordt uitsluitend bij incidenten of op ad hoc basis overlegd.

Waar is het onderwerp privacy binnen uw organisatie primair belegd?



Hoe vaak komen Business, Legal en IT (Security) bij elkaar om privacy zaken te bespreken?



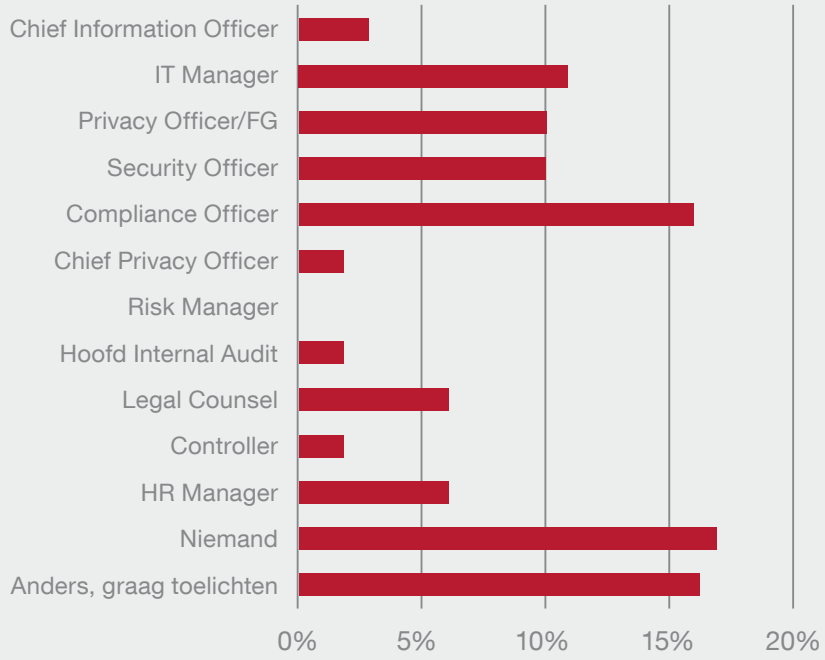
Privacy in uw organisatie

Organisaties beleggen de verantwoordelijkheid voor het onderwerp privacy bij verschillende rollen.

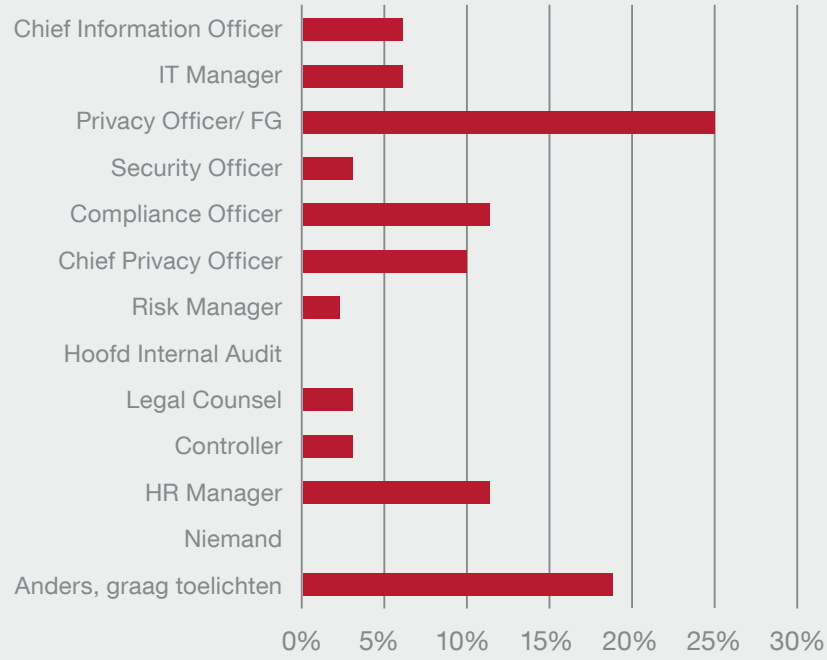
In ***17%*** van de gevallen is de verantwoordelijkheid voor het privacybeleid niet belegd.

De vraag waar de verantwoordelijkheid voor het privacybeleid behoort te liggen levert eveneens een diffuus beeld op. Ruim een derde ***(35%)*** geeft aan dat deze verantwoordelijkheid thuishoort bij de (Chief) Privacy Officer of de Functionaris Gegevensbescherming (FG).

Wie is er op dit moment binnen uw organisatie verantwoordelijk voor de implementatie van het privacybeleid?



Wie zou er naar uw oordeel verantwoordelijk moeten zijn voor het privacybeleid binnen uw organisatie?



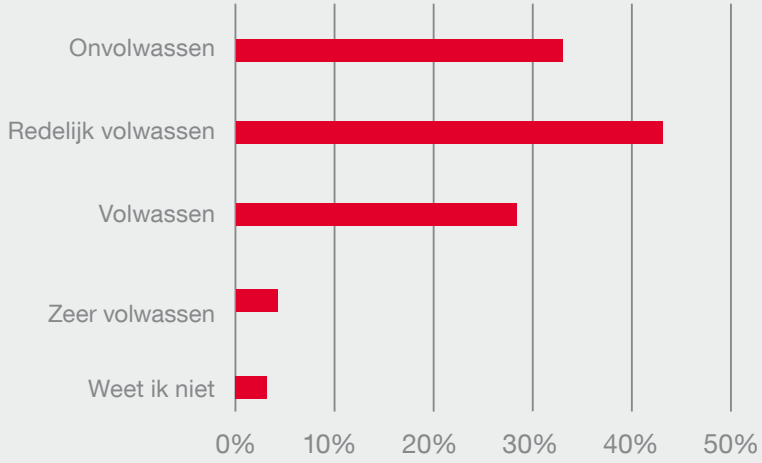
Privacy Strategie en Beleid

Slechts ***22%*** van de respondenten geeft aan dat de omgang met persoonsgegevens binnen de eigen organisatie (zeer) volwassen is.

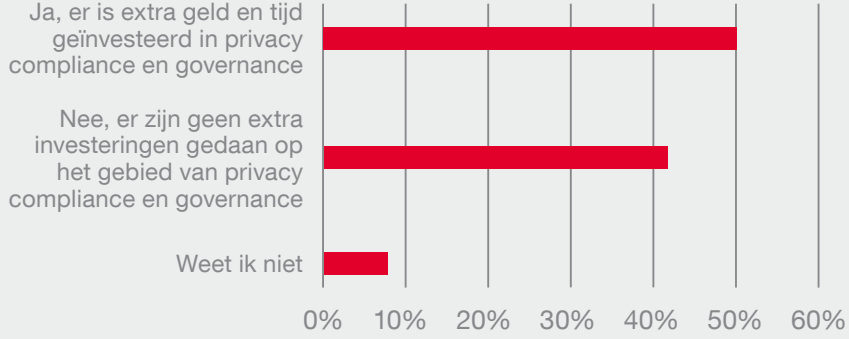
Tegen ***een derde*** die de omgang met persoonsgegevens in de eigen organisatie onvolwassen acht.

Bij ***50%*** van de organisaties zijn gedurende het afgelopen jaar extra investeringen gedaan op het gebied van privacy compliance en governance.

Hoe volwassen (ontwikkeld) is naar uw mening de omgang met persoonsgegevens binnen uw organisatie (inclusief koppeling met strategie rapportagevereisten en privacybeleid)?



Heeft uw organisatie het afgelopen jaar extra geïnvesteerd in privacy compliance en governance?

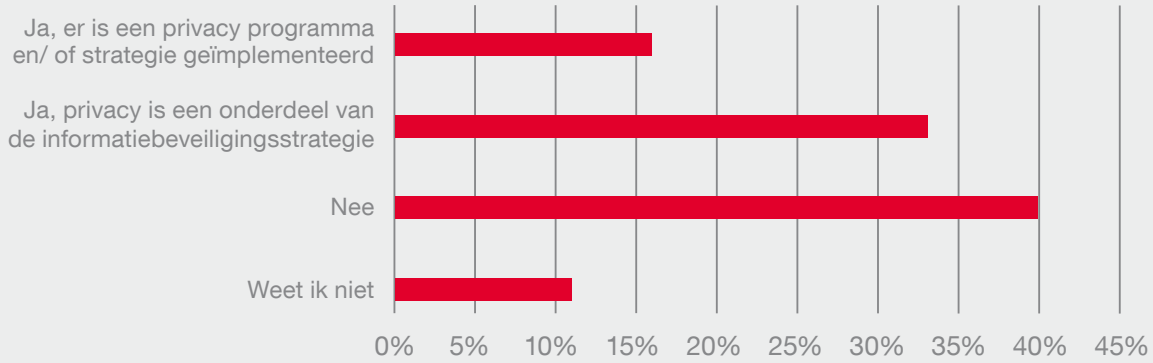


Privacy Strategie en Beleid

Bij de ***helft*** van de organisaties is er een privacy programma en/ of strategie geïmplementeerd. Dit is grofweg gelijk aan de resultaten van vorig jaar.

40% van de deelnemende organisaties is geen sprake van een privacy programma of strategie op het gebied van privacy.

Heeft uw organisatie een privacy programma en/ of strategie geïmplementeerd?

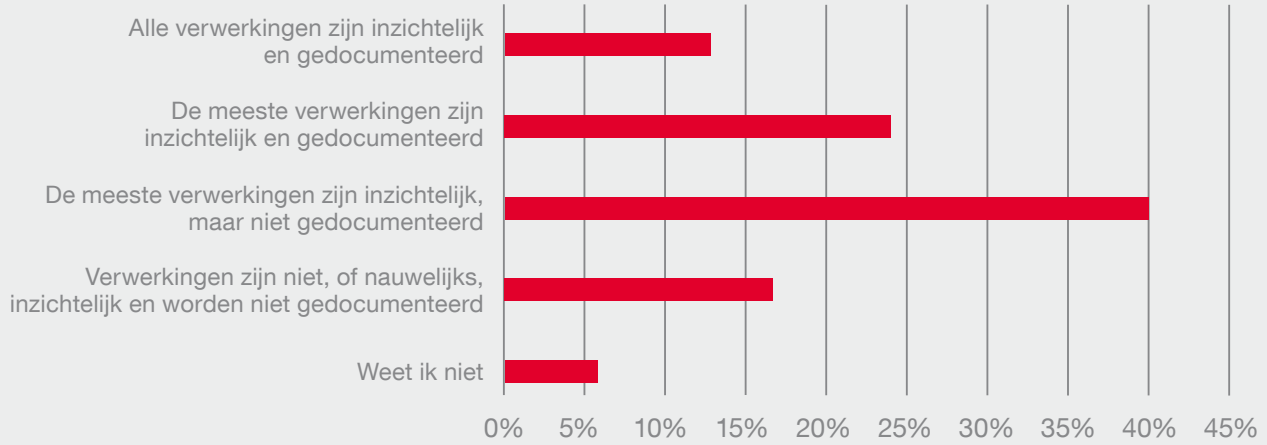


Privacy Strategie en Beleid

De Algemene Verordening Gegevensbescherming stelt het organisaties verplicht een gedetailleerde beschrijving van de bewerkingen van persoonsgegevens op te stellen en bij te houden.

Slechts ***13%*** van de organisaties voldoet aan de voorwaarde uit de Algemene Verordening Gegevensbescherming om alle verwerkingen van persoonsgegevens te documenteren. Bij een ruime meerderheid zijn verwerkingen van persoonsgegevens niet of nauwelijks gedocumenteerd.

Heeft uw organisatie inzichtelijk en gedocumenteerd welke persoonsgegevens worden verwerkt?



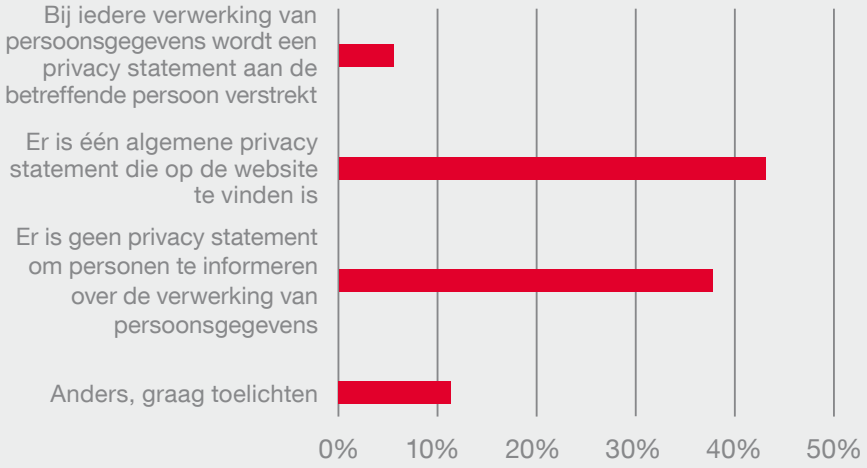
Privacy Strategie en Beleid

Bij slechts ***50%*** van de deelnemende organisaties vindt transparante communicatie over de verwerking van persoonsgegevens plaats via een privacy statement.

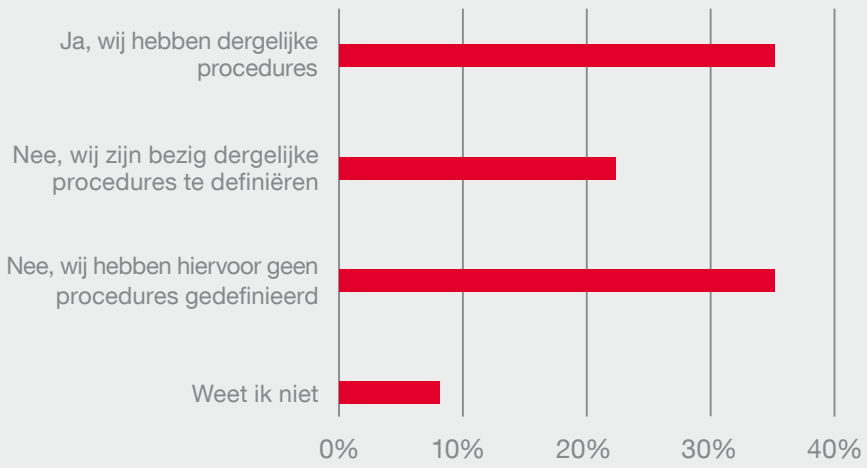
Bijna ***40%*** van de deelnemers hanteert geen privacy statement op de website van de organisatie.

Ruim ***een derde*** van de organisaties heeft procedures voor de afhandeling van inzage- en correctieverzoeken geïmplementeerd, ***22%*** is bezig dergelijke procedures te definiëren en te implementeren.

Op welke manier zorgt uw organisatie voor een transparante communicatie richting personen over het verwerken van zijn of haar persoonsgegevens?



Heeft uw organisatie inzage- en correctieprocedures om verzoeken van betrokkenen af te handelen?

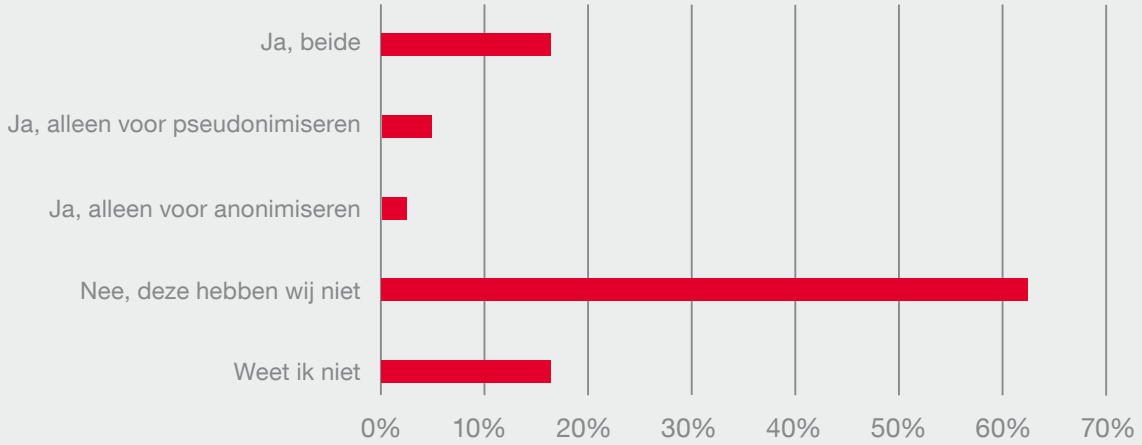


Privacy Strategie en Beleid

Bij ***62%*** van de deelnemende organisaties is geen sprake van beleid op het gebied van pseudonimiseren en/of anonimiseren van persoonsgegevens.

Slechts ***16%*** voert beleid zowel inzake pseudonimiseren als anonimiseren.

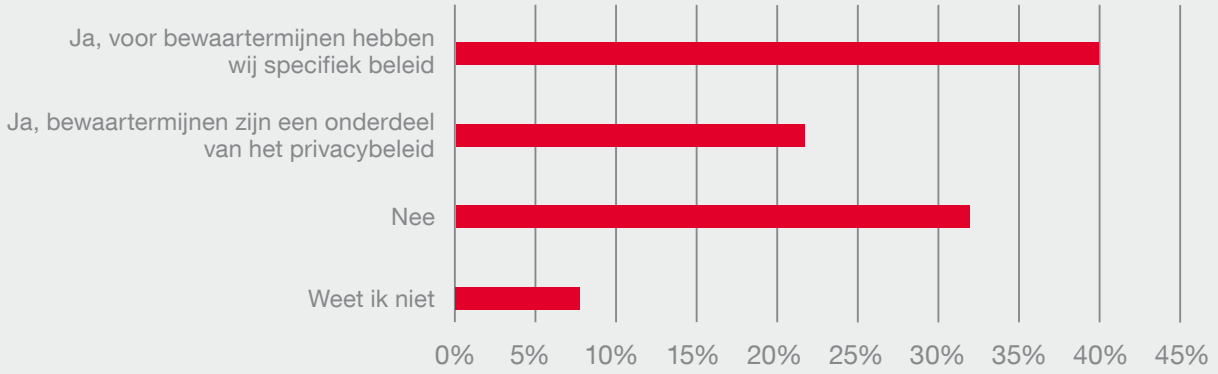
Heeft uw organisatie beleid inzake het pseudonimiseren (identificerende gegevens vervangen door versleutelde gegevens) en/ of anonimiseren (anoniem maken) van persoonsgegevens?



Privacy Strategie en Beleid

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

Heeft uw organisatie beleid inzake het bewaren en verwijderen van persoonsgegevens?

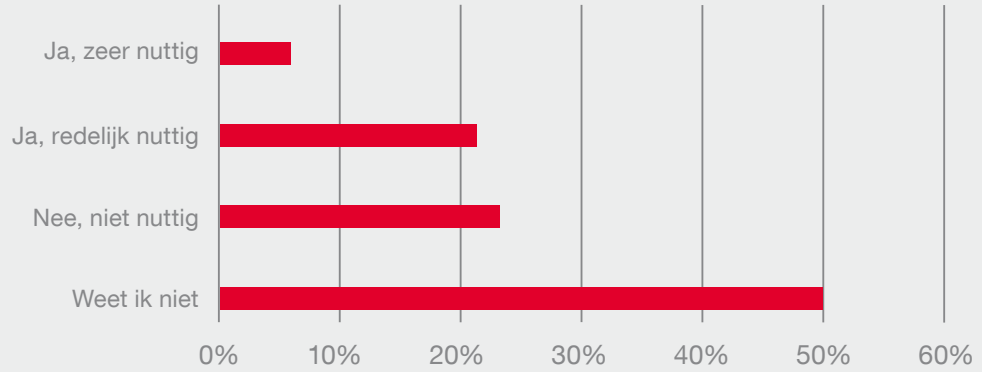


Privacy Strategie en Beleid

De Algemene Verordening Gegevensbescherming introduceert het Europese Data Privacy Protection Seal.

Slechts ***27%*** van de respondenten denkt dat het voor de eigen organisatie nuttig kan zijn om een dergelijk Seal te halen.

Denkt u dat het voor uw organisatie nuttig is om een dergelijk data privacy Protection Seal te halen?



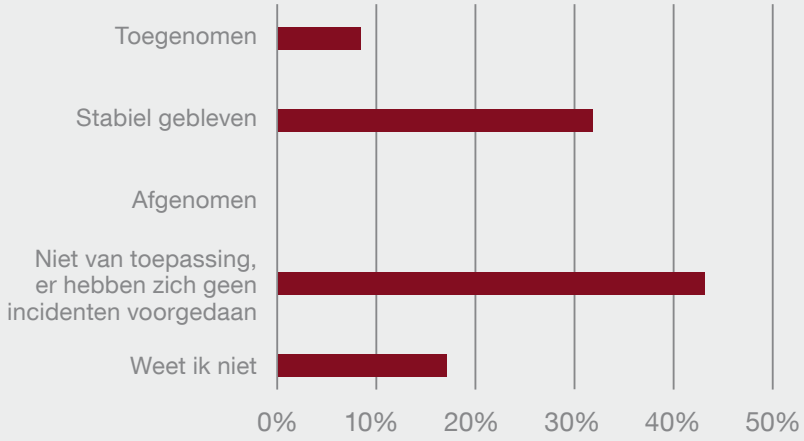
Privacy incidenten en meldingen

43% van de respondenten geeft aan dat er zich bij de eigen organisatie het afgelopen jaar geen privacy incidenten hebben voorgedaan.

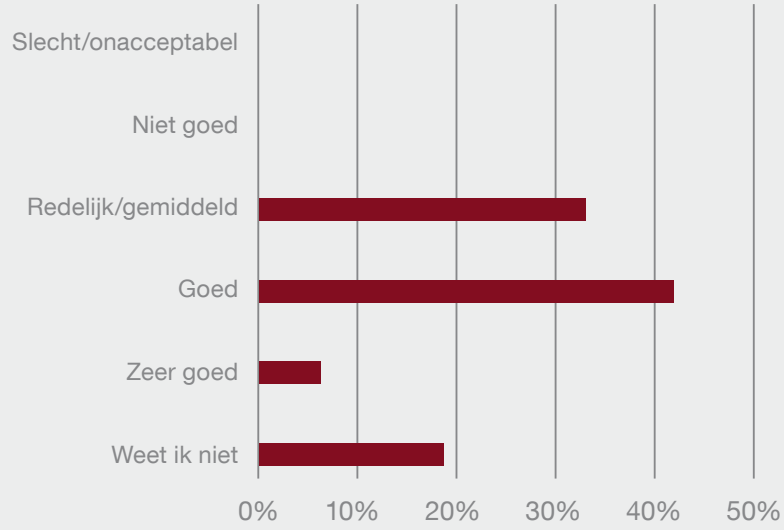
In slechts ***8%*** van de gevallen is sprake van een toename van het aantal privacy incidenten.

Bijna de ***helft*** van de deelnemers geeft aan dat de eigen organisatie goed tot zeer goed heeft gereageerd op privacy incidenten die zich hebben voorgedaan.

Is het aantal privacy incidenten, voor zover u weet, toe- of afgenomen in het afgelopen jaar?



Hoe heeft uw organisatie, naar uw oordeel, gereageerd op de privacy incidenten?



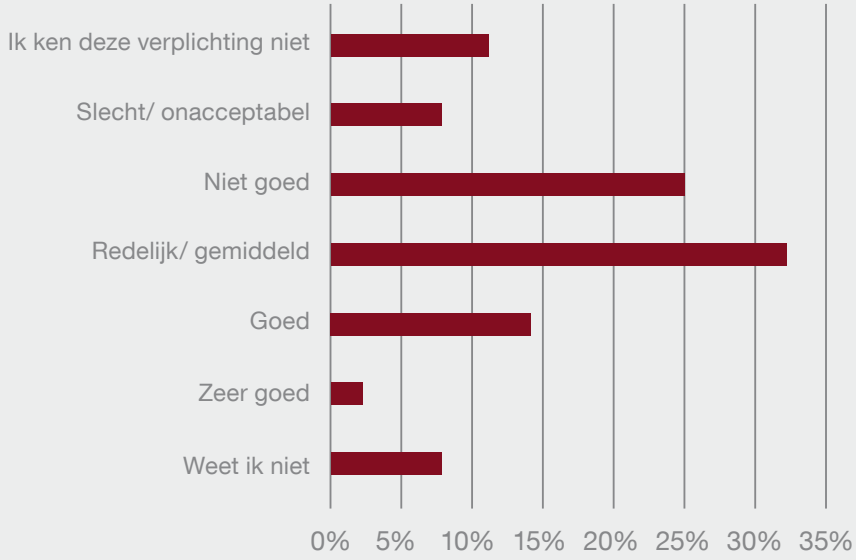
Privacy incidenten en meldingen

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.

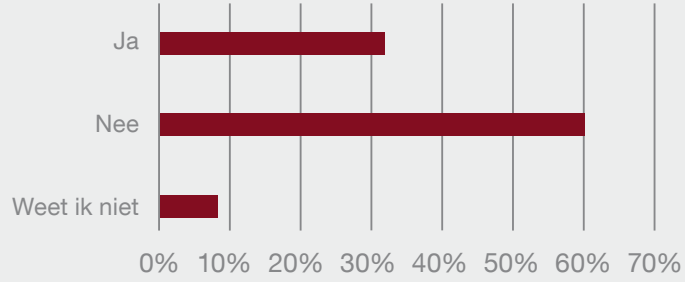
11% van de respondenten is nog niet bekend met de verplichtingen uit de Wet Meldplicht Datalekken. Daarnaast geeft een ***derde*** van de organisaties aan nog niet goed voorbereid te zijn op deze verplichtingen.

Slechts ***32%*** van de organisaties heeft een communicatieplan geïmplementeerd voor het geval er zich een datalek voordoet.

Vindt u dat uw organisatie goed is voorbereid om aan deze verplichtingen te voldoen?



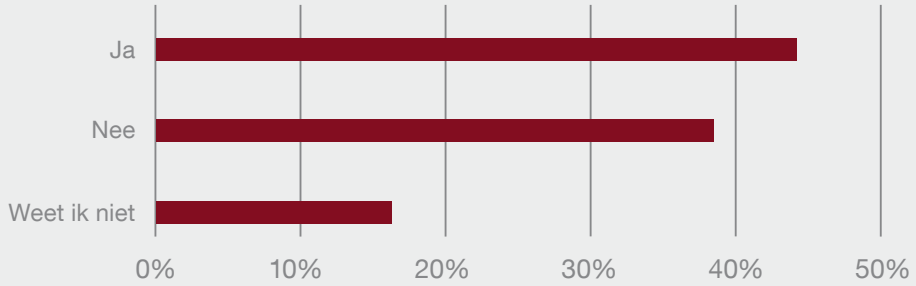
Heeft uw organisatie een communicatieplan voor het geval er zich een datalek voordoet?



Privacy incidenten en meldingen

Minder dan de ***helft*** van de organisaties voldoet aan de wettelijke verplichting om een centraal overzicht bij te houden van datalekken die zich in de organisatie voordoen.

Houdt uw organisatie een overzicht bij van datalekken?

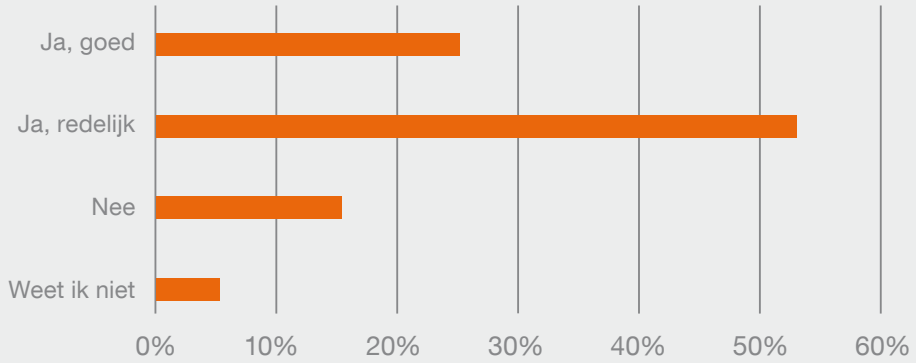


Privacy en uw leveranciers

Ongeveer ***twee derde*** van de deelnemers geeft aan dat de eigen organisatie, ondanks haar verantwoordelijkheid, niet of slechts redelijk zicht heeft op datastromen naar externe partijen.

Slechts ***25%*** van de respondenten geeft aan dat dit wel goed inzichtelijk is.

Heeft uw organisatie als geheel vanuit privacy oogpunt goed inzicht in de datastromen betreffende persoonsgegevens tussen uw organisatie en externe partijen (leveranciers, klanten, gegevensbewerkers)?



Privacy en uw leveranciers

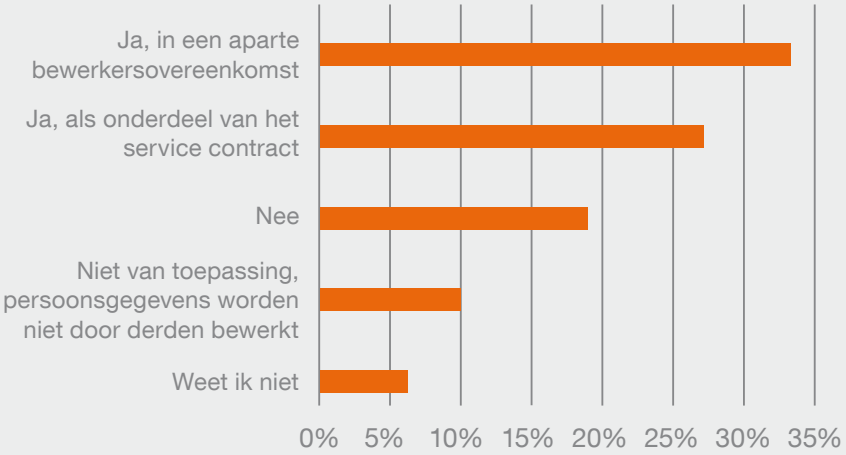
Op basis van de Wet bescherming persoonsgegevens is het verplicht om contractuele verplichtingen op te leggen aan externe partijen (bijv. leveranciers) die in uw opdracht persoonsgegevens verwerken. Als organisatie kunt u ervoor kiezen om deze verplichtingen in bestaande contracten te verwerken of separaat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

Door ***een derde*** van de organisaties worden contractuele verplichtingen met bewerkers van persoonsgegevens vastgelegd in aparte bewerkersovereenkomsten.

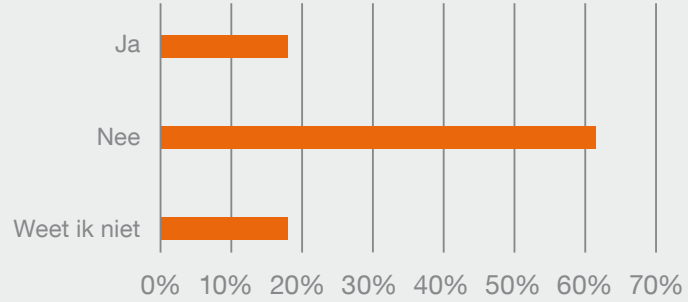
Bijna ***25%*** van de organisaties legt contractuele verplichtingen inzake omgang met persoonsgegevens in zijn geheel niet vast.

Een grote meerderheid van de organisaties ***(63%)*** controleert de bewerkersovereenkomsten niet periodiek op naleving.

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



Controleert u de bewerkersovereenkomsten periodiek op naleving (of laat u deze periodiek controleren)?



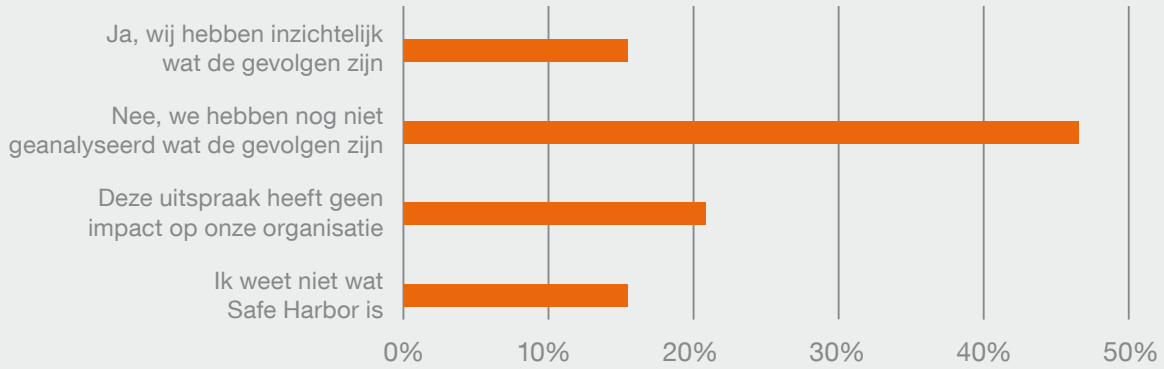
Privacy en uw leveranciers

Het Europees Hof van Justitie heeft op 6 oktober 2015 het Safe Harbor-verdrag met de Verenigde Staten (VS), dat als juridische waarborg gold voor de doorgifte van persoonsgegevens naar de VS, ongeldig verklaard.

Bijna ***de helft*** van de respondenten geeft aan dat er nog geen analyse is gemaakt inzake de gevolgen van de Safe Harbor uitspraak voor de eigen organisatie. Dit terwijl er wel gegevens worden uitgewisseld met de VS.

Slechts ***16%*** geeft aan wel inzichtelijk te hebben wat hiervan de gevolgen zijn voor de eigen organisatie.

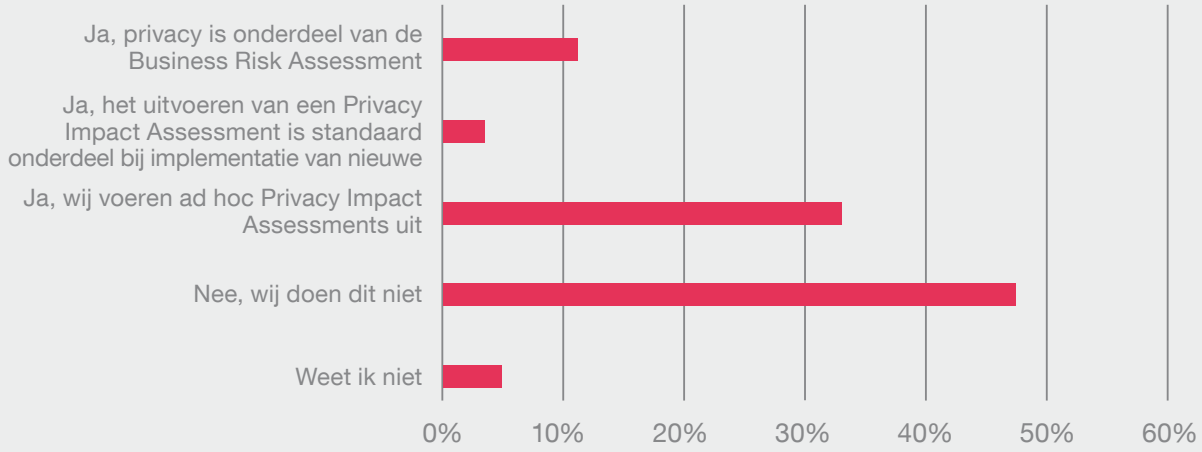
Heeft uw organisatie inzichtelijk wat de gevolgen zijn van het ongeldig verklaren van Safe Harbor?



Uw organisatie en het privacyrisico

Bijna ***de helft*** van de deelnemende organisaties geeft aan geen risicoanalyses uit te voeren in het kader van omgang met persoonsgegevens. ***Een derde*** doet dit uitsluitend op ad hoc basis.

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



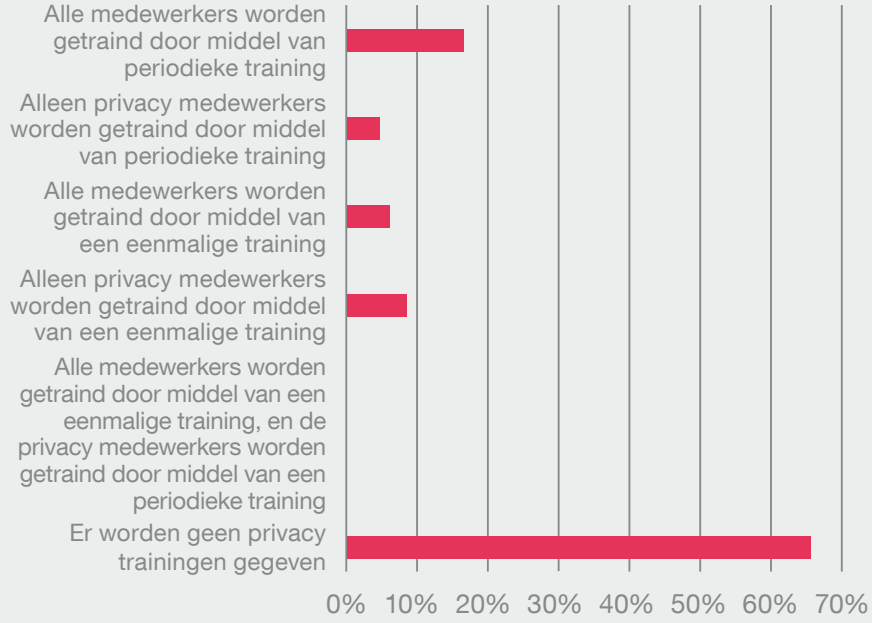
Uw organisatie en het privacyrisico

Door bijna ***een derde*** van de organisaties wordt compliance aan de Wet bescherming persoonsgegevens periodiek beoordeeld, al dan niet als onderdeel van een auditcyclus.

Bij ***65%*** van de organisaties heeft het personeel in de afgelopen 12 maanden geen training of opleiding op het gebied van privacy gevolgd.

Worden privacy en compliance aan de Wet bescherming persoonsgegevens (Wbp) periodiek beoordeeld?

Hoe worden uw medewerkers getraind op het gebied van privacy?

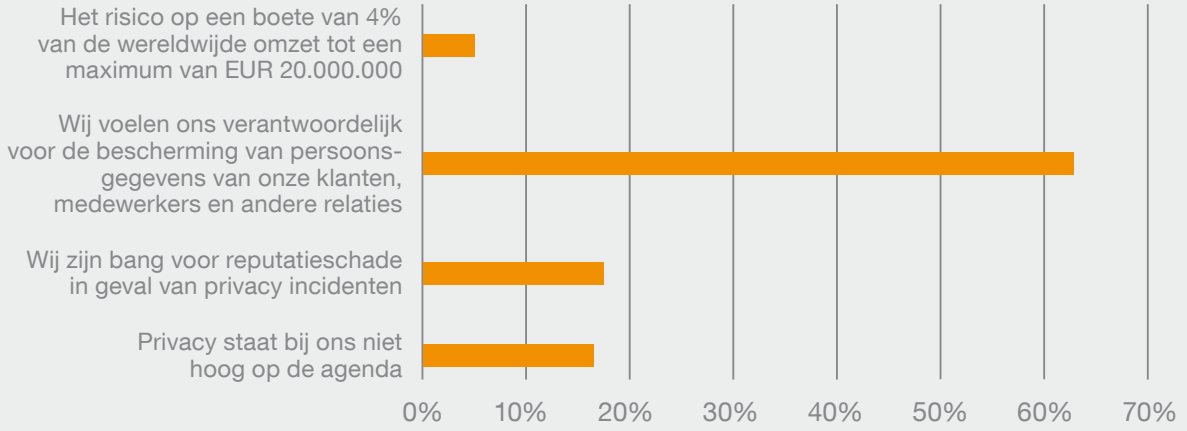


Stellingen

Voor een ruime meerderheid ***(62%)*** van de organisaties is de bescherming van de persoonsgegevens van klanten, personeel en andere relaties de belangrijkste reden om het onderwerp privacy hoog op de agenda te zetten.

Bij slechts een gering aantal organisaties ***(5%)*** is het onder de aanstaande Algemene Verordening Gegevensbescherming versterkte boeteregime de belangrijkste reden.

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

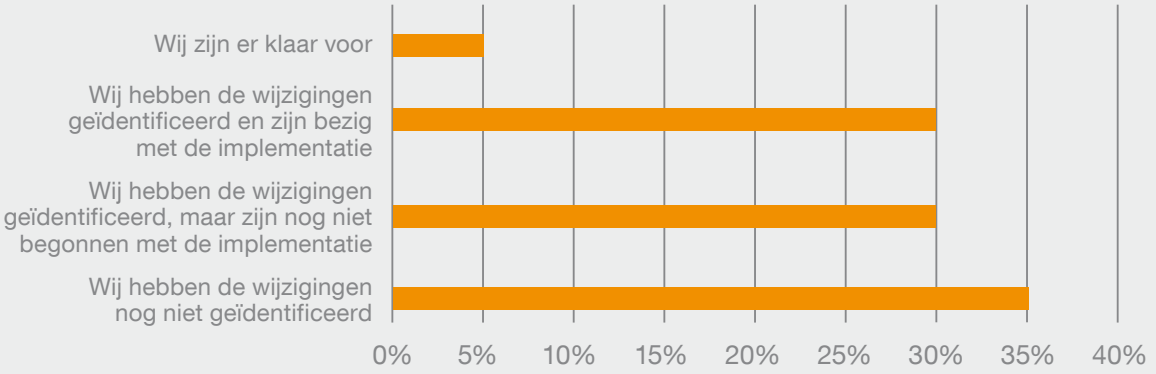


Stellingen

Ruim ***een derde*** van de deelnemende organisaties geeft aan dat het de toekomstige wijzigingen in privacyregelgeving nog niet heeft geïdentificeerd.

Slechts ***5%*** zegt klaar te zijn voor de gewijzigde privacy regelgeving.

Wij zijn klaar voor de wijzigingen in de privacy regelgeving (Algemene Verordening Gegevensbescherming / Wet Meldplicht Datalekken):

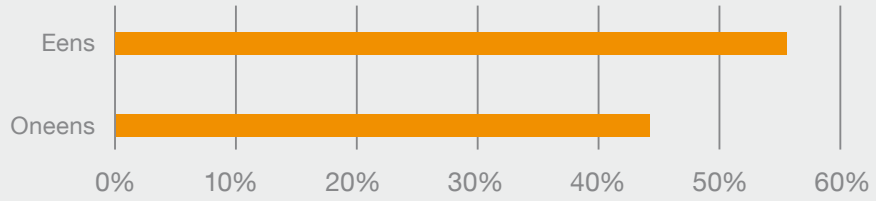


Stellingen

Op basis van de Algemene Verordening Gegevensbescherming 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 ***44%*** van de deelnemende organisaties aan hier bij de ontwikkeling van nieuwe systemen niet altijd rekening mee te houden.

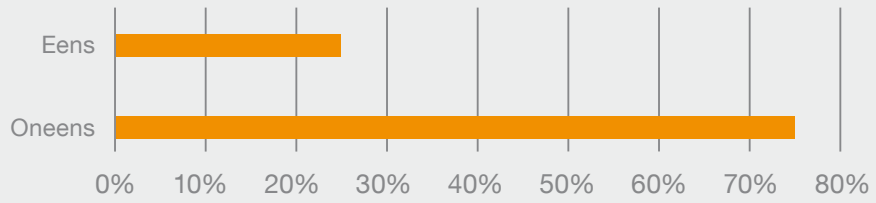
Bij implementatie van nieuwe systemen houden wij altijd in een vroeg stadium rekening met privacy aspecten en de bescherming van persoonsgegevens (Privacy by Design principe):



Stellingen

25% van de respondenten ervaart privacyregelgeving als belemmerend voor de innovatiemogelijkheden van de organisatie.

Privacyregelgeving beperkt onze innovatiemogelijkheden:

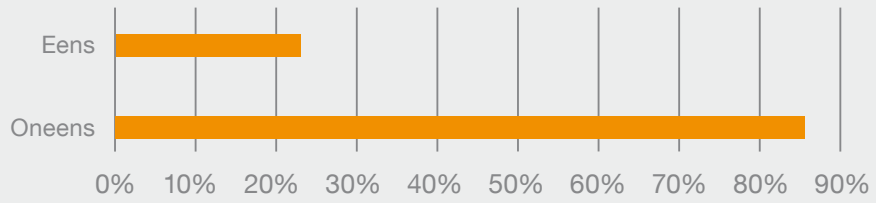


Stellingen

De wijze van omgang met persoonsgegevens en privacy van relaties kan door organisaties worden gebruikt om zich te profileren en te onderscheiden van de concurrentie.

Slechts ***14%*** van de organisaties benut het privacybeleid om zich te onderscheiden in de markt.

Wij gebruiken privacy en ons privacy beleid om ons te profileren en te onderscheiden in de markt:

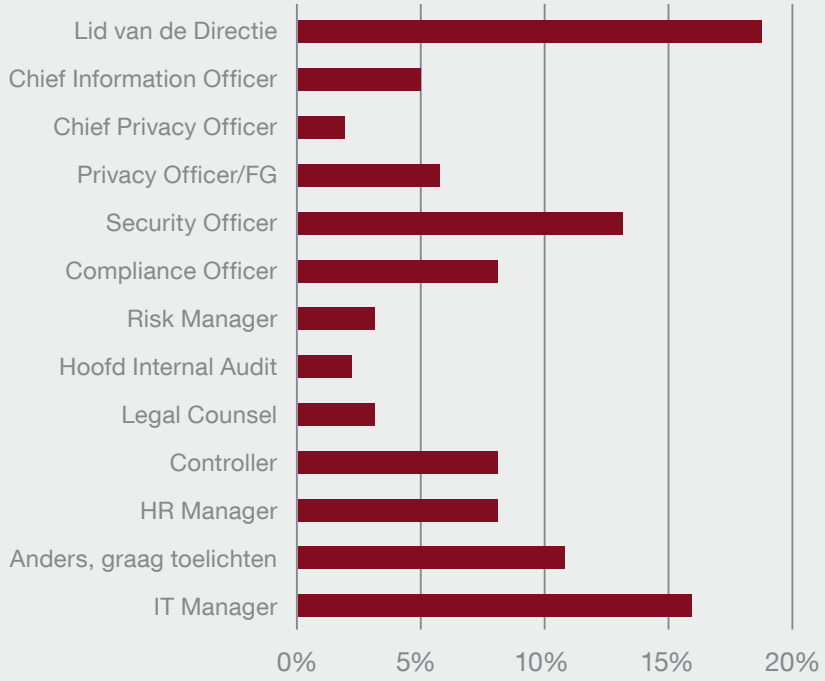


Over u en uw organisatie

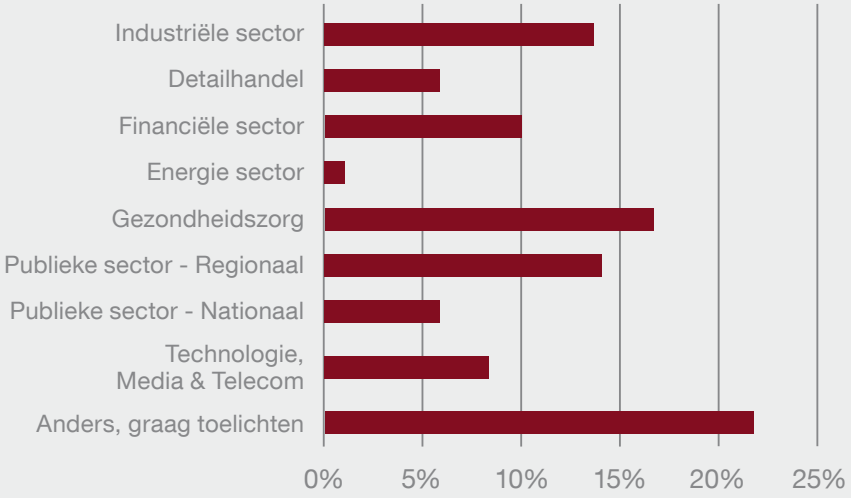
De individuele respondenten van de survey zijn werkzaam in een grote verscheidenheid aan functies.

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

Welke van deze functietitels beschrijft uw rol het beste?



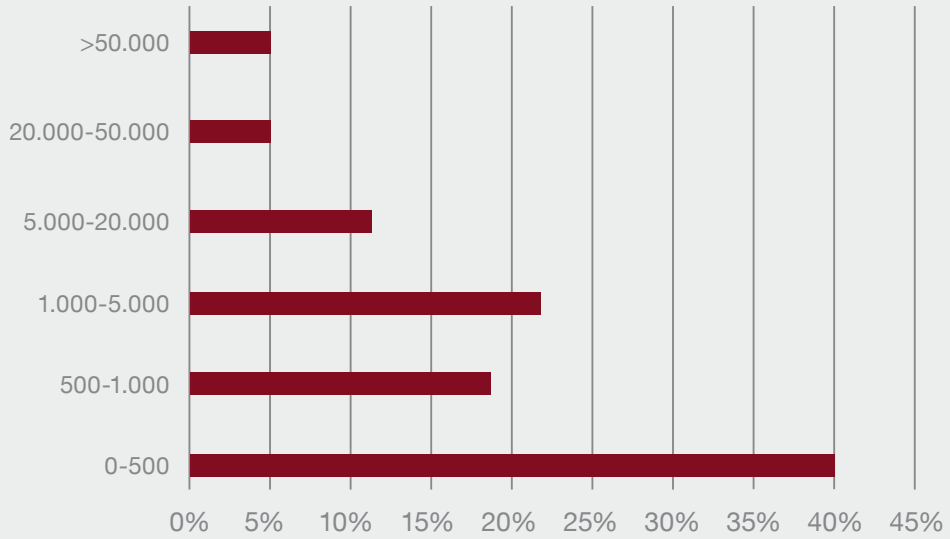
Welke sectorclassificering is het meest van toepassing op de belangrijkste activiteiten van uw organisatie?



Over u en uw organisatie

40% van de deelnemende organisaties heeft minder dan 500 werknemers.
21% van de organisaties heeft tussen de 1.000 en 5.000 werknemers en ***5%*** heeft meer dan 50.000 werknemers.

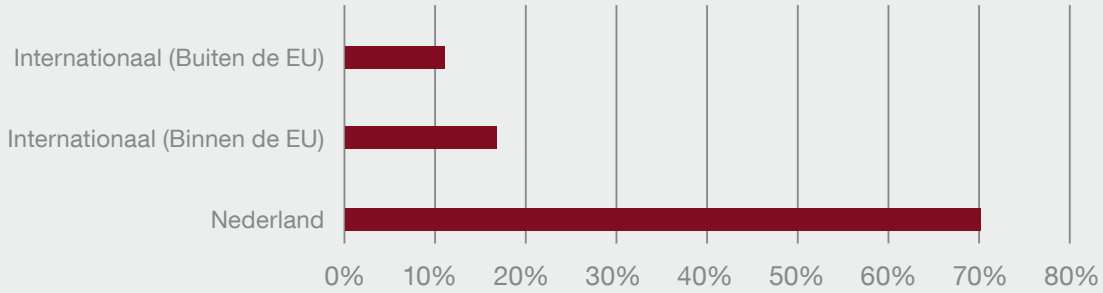
Hoeveel werknemers heeft uw organisatie wereldwijd?



Over u en uw organisatie

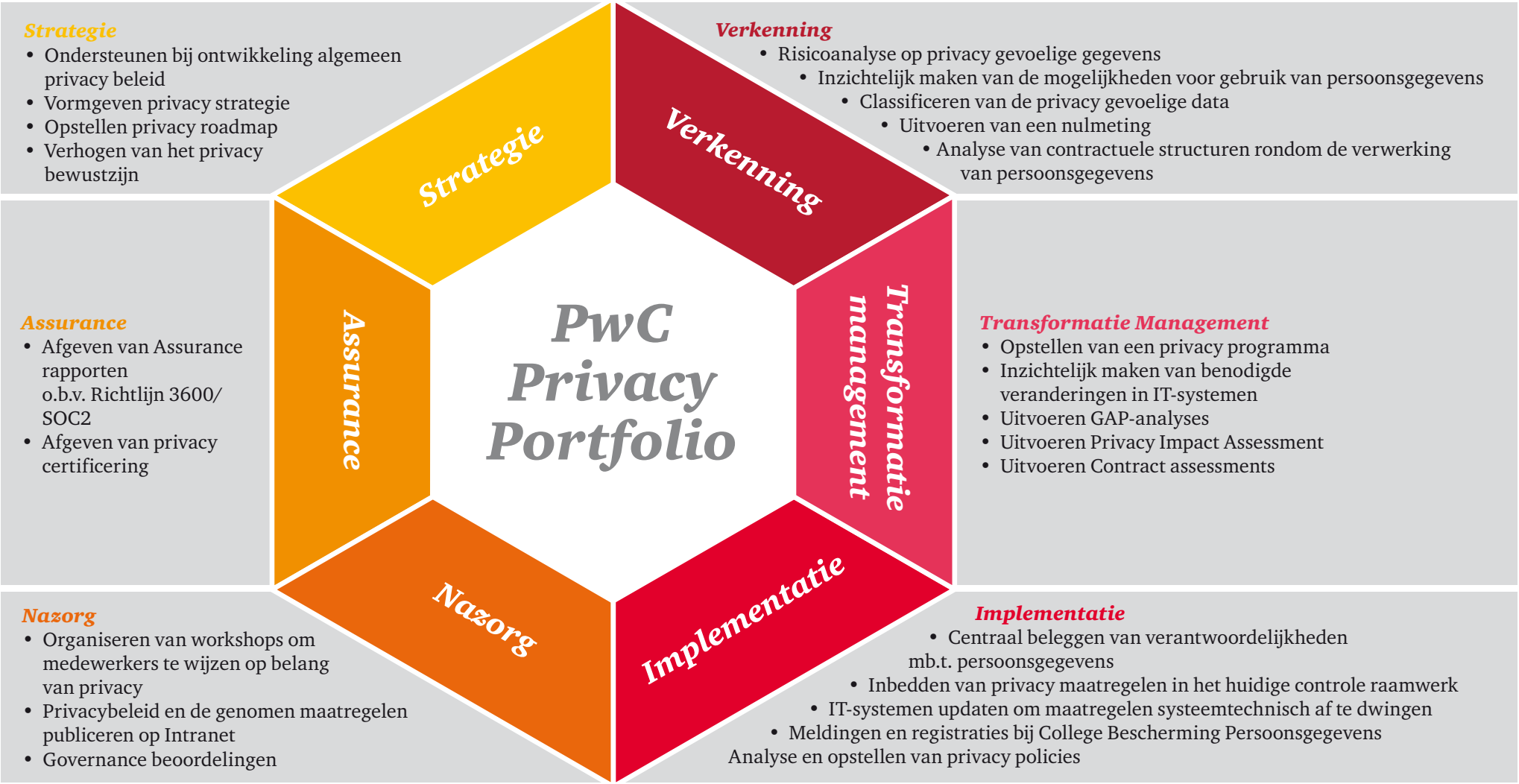
Bij ***70%*** van de deelnemende organisaties zijn de activiteiten voornamelijk op Nederland gericht.

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



Bijlagen

Bijlage A: Privacy Portfolio van PwC



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. Richtlijn 3600/ SOC2
- Afgeven van privacy certificering

Transformatie Management
- 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 College Bescherming 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 Technology and Security
+31 (0)88 792 53 88
bram.van.tiel@nl.pwc.com

https://www.linkedin.com/in/bramvantiel

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

https://nl.linkedin.com/in/yvette-van-gemerden-04b839

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

www.pwc.nl/privacy