NETWORK

Evaluatie Implementatie AVG mei 2019

Voorwoord

Met DPO Network wil de NHB haar klanten een betrouwbare en onafhankelijke kennispartner bieden voor AVG compliance en implementatie vraagstukken in de financiële dienstverlening. De NHB onderschrijft hiermee het belang van privacy en goede gegevensbescherming voor klanten en voor het imago van de sector.

Om een inzicht te krijgen waar financieel dienstverleners en intermediairs staan met hun implementatie van de AVG hebben we klanten van de NHB gevraagd hebben mee te werken aan de enquête Evaluatie Implementatie AVG. Waarvoor onze dank!

Voor DPO Network is het van belang om te weten waar u staat, welke vragen er leven, waar behoefte aan is, welke risico's er mogelijk zijn en waar aandacht aan besteed zouden moeten worden. Meten is weten.

Het in werking treden van de Algemene Verordening Gegevensbescherming is het afgelopen jaar niet ongemerkt voorbij gegaan. Zo heeft de Autoriteit Persoonsgegevens (de Nederlandse gegevensbeschermingsautoriteit) een duidelijk begin gemaakt met het uitvoering geven aan haar toezichthoudende taak en boetebevoegdheid. Een jaar na het in werking treden van de AVG is dan ook een goed ijkmoment om te kijken waar we staan.

De uitkomst van de enquête geeft een aantal interessante inzichten. Duidelijk komt naar voren dat voldoen aan de AVG een actueel onderwerp is.

Is het u gelukt om aan de vereisten die de AVG aan uw beroepspraktijk stelt te voldoen? Voor wie doet u het eigenlijk? Is het de inspanning waard? Staan de inspanning in verhouding tot uw primaire werkzaamheden?

Met de uitkomst van deze evaluatie hopen we inzichtelijk te kunnen maken waar u staat ten opzichte van vergelijkbare organisaties, welke zaken mogelijk aandacht verdienen en waar de kansen liggen die de AVG uw organisatie biedt.

Amsterdam, 23 mei 2019,
namens DPO Network,

Jan van den Berg
Gerrit van Rooij

1. In hoeverre bent u op de hoogte van de verplichtingen die de AVG met zich meebrengt?

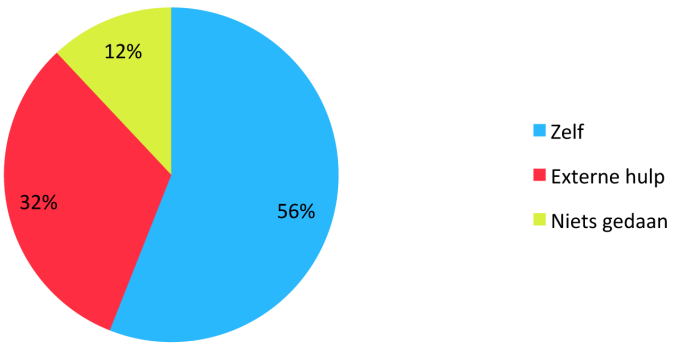
De AVG is vorig jaar mei effectief geworden. Om bedrijven te informeren over de nieuwe regels is in de sector veel aan informatieverstrekking gedaan. O.a. door leveranciers (bijv. de Nationale Hypotheekbond) en brancheorganisaties (AdFiz).

Ook de Autoriteit Persoonsgegevens en het Ministerie van Justitie en Veiligheid zijn op dit vlak actief geweest. Dit heeft er toe geleid dat de meeste bedrijven redelijk tot goed op de hoogte zijn van de verplichtingen.

2. Op welke wijze bent u met de AVG aan de slag gegaan?

De meeste respondenten zijn aan de slag gegaan met bestaande templates die in de branche o.a. door DPO Network en AdFiz ter beschikking zijn gesteld. Een derde heeft daarbij externe hulp ingeroepen.

Meer dan 1 op de 10 respondenten heeft echter niets gedaan.

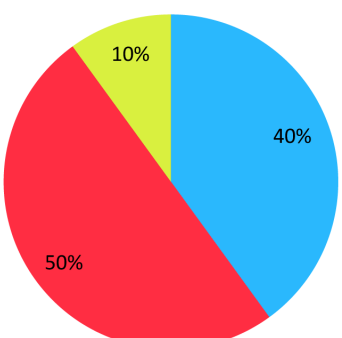


56%	Zelf (handleidingen en formats)
32%	Externe hulp (handleidingen en formats)
12%	Niets gedaan

3. Hoever bent u op dit moment met het implementeren van de AVG-verplichtingen?

Van respondenten zegt 6 op de 10 nog niet klaar te zijn met de implementatie van de AVG. Dit terwijl de Autoriteit Persoonsgegevens in toenemende mate klaar is om handhavend op te treden.

De overige respondenten geven aan alles voldoende op orde te hebben.



Voldoende geïmplementeerd

Bezig met implementatie

Moeten nog beginnen

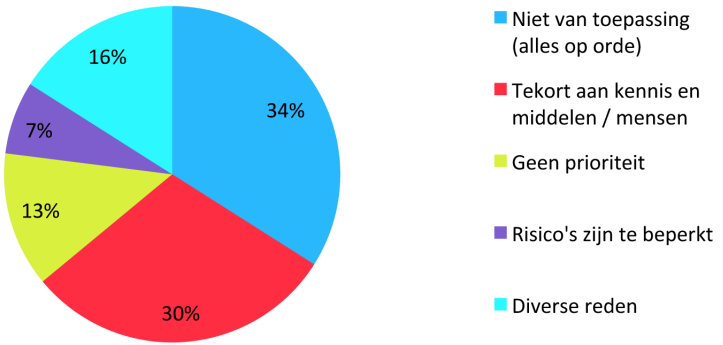
40%	Voldoende geïmplementeerd
50%	Bezig met implementatie
10%	Nog niet begonnen

4. Als u de verplichtingen nog niet voldoende geïmplementeerd heeft, wat zijn dan de redenen daarvoor?

Het beeld uit vraag 3, dat ca. 40% van de respondenten aangeeft op orde te zijn met implementatie van de AVG, wordt hier niet geheel bevestigd.

Uit respons op vraag 4 blijkt namelijk dat 66% (het overgrote deel) aangeeft de AVG niet voldoende te hebben geïmplementeerd.

Redenen hiervoor lopen in volgorde van belangrijkheid uiteen van: tekort aan personeel, geen prioriteit of dat de risico's te beperkt zijn om er iets aan te gaan doen. Bij diverse redenen wordt o.a. aangegeven dat er duidelijkheid in regelgeving ontbreekt, er geen goede model-documenten voor handen zijn en dat er twijfels zijn over digitaal werken.

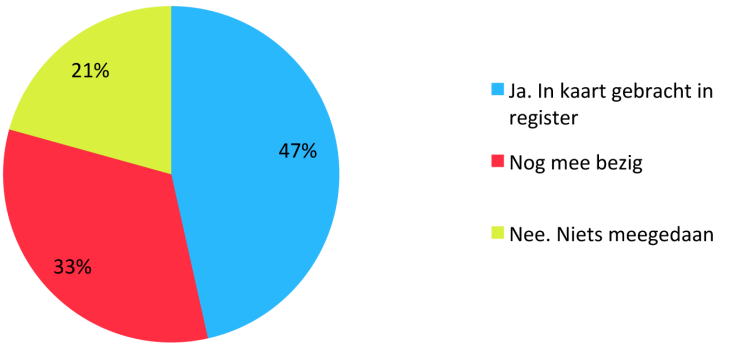


34%	Niet van toepassing (alles op orde)
30%	Tekort aan kennis en middelen / mensen
13%	Geen prioriteit
7%	Risico's zijn te beperkt
16%	Diverse redenen

5. Weet u welke persoonsgegevens (en in welke systemen) u verwerkt, en heeft u deze in een verplicht verwerkingsregister opgenomen?

Het verwerkingsregister waarin het overzicht van het verwerken van persoonsgegevens wordt gemaakt, wordt gezien als de basis van AVG compliance. Uit de antwoorden blijkt dat een overgroot deel van de respondenten dit overzicht heeft of bezig is deze op te stellen.

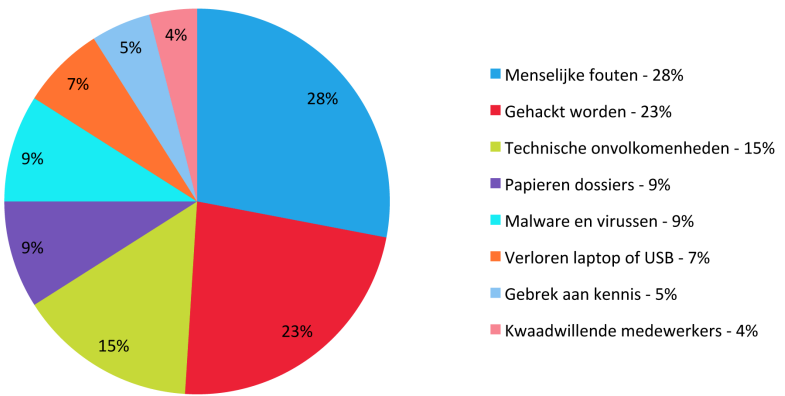
Nog altijd heeft één op de vijf respondenten niet de essentiële gegevens in kaart gebracht die nodig zijn om de AVG verplichtingen na te komen.



47 %	Ja. In kaart gebracht in register
33 %	Nog mee bezig
21 %	Nee. Niets meegedaan

6. Wat ziet u binnen uw organisatie als grootste risico of bedreiging van privacy en de beveiliging van persoonsgegevens die u verwerkt?

Deze resultaten ontkrachten het idee dat technische maatregelen afdoende zijn om persoonsgegevens te beschermen. Onzorgvuldig menselijk handelen ligt aan de basis van het overgrote deel van de door respondenten benoemde risico's en is daarmee de belangrijkste bedreiging van privacy en de beveiliging van persoonsgegevens.



28%	Menselijke fouten
23%	Gehackt worden
15%	Technische onvolkomenheden
9%	Papieren dossiers
9%	Malware en virussen
7%	Verloren laptop of USB
5%	Gebrek aan kennis
4%	Kwaadwillende medewerkers

7. Heeft u sinds mei 2018 verzoeken van klanten of medewerkers gehad tot inzage, het wissen of het overdragen van persoonsgegevens die u van hen verwerkt?

In toenemende mate stellen consumenten eisen aan de omgang met persoonsgegevens. Hierbij past dat ze vaker verzoeken indienen om persoonsgegevens in te zien, ze te laten wissen of over te dragen. Uit de enquête blijkt dat een kwart van de respondenten het afgelopen jaar te maken heeft gehad met verzoeken van consumenten. Van belang is dan ook dat ze hun zaken op orde hebben om tijdig en volledig op de verzoeken in te gaan.

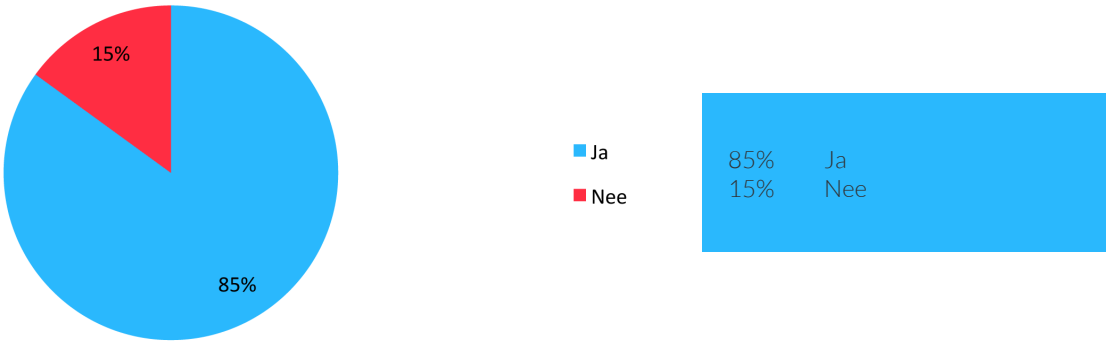
Als er verzoeken binnen kwamen ging het in de meeste gevallen om verzoeken om gegevens te wissen, gevolgd door die om gegevens in te zien of over te dragen.

8. Verwerkt u in het kader van uw dienstverlening het BSN van uw klanten?

Het burgerservicenummer (BSN) is primair bedoeld voor het contact tussen burgers en de overheid. Organisaties buiten de overheid mogen het BSN alleen gebruiken *" ter uitvoering van de wet dan wel voor doeleinden bij wet bepaald"*.

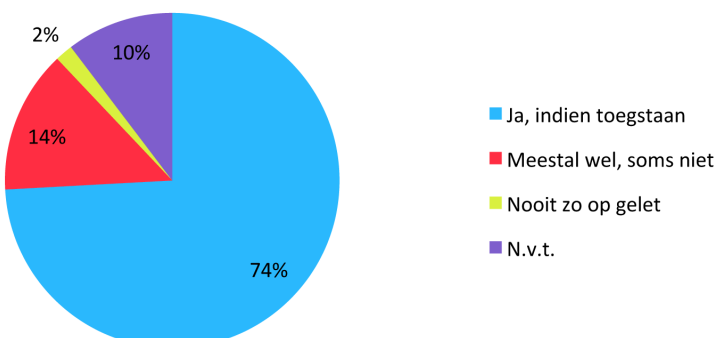
Het BSN mag dus alleen worden verwerkt voor doeleinden die per wet bepaald zijn. In sommige situaties moet je als financieel adviseur het BSN dus verwerken.

Uiteraard schrijft de wet niet voor dat de onafhankelijk financieel adviseur in die situaties een rol móet hebben. Logischerwijs geeft de wet de adviseur dan ook geen wettelijke plicht om het BSN te verwerken.



9. Indien u het BSN van uw klanten verwerkt, heeft u dan het idee dat dit rechtmatig gebeurt?

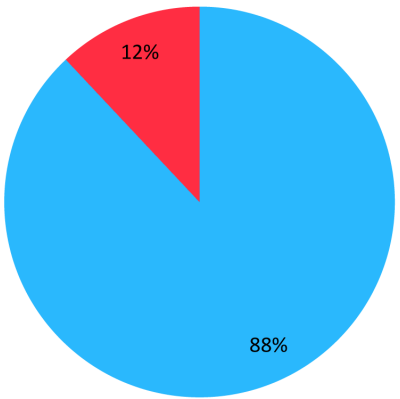
De AP benadrukt echter ook dat als de adviseur het BSN mag verwerken voor (de aanvraag van) een bepaald financieel product dit niet betekent dat hij het BSN voor andere doelen, zoals zijn eigen administratie, mag gebruiken.

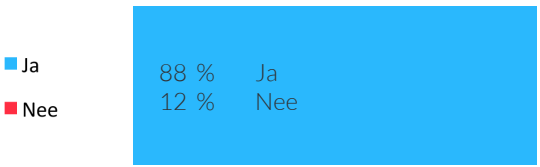


74%	Ja, indien toegestaan
14%	Meestal wel, soms niet
2%	Nooit zo op gelet
10%	N.v.t.

10. Heeft u maatregelen genomen om kennis en bewustzijn bij medewerkers over privacy en het omgaan met persoonsgegevens te verhogen?

De meeste financiële dienstverleners geven aan maatregelen te hebben genomen om kennis en bewustzijn bij medewerkers te vergroten.
Uit vraag 6 blijkt dat menselijke fouten als grootste privacy risico worden aangemerkt. Ook de jaarrapportage 2018 van de Autoriteit Persoonsgegevens laat zien dat de meeste datalekken menselijke fouten als oorzaak hebben. In dat licht valt op dat 12% aangeeft geen maatregelen te hebben getroffen.





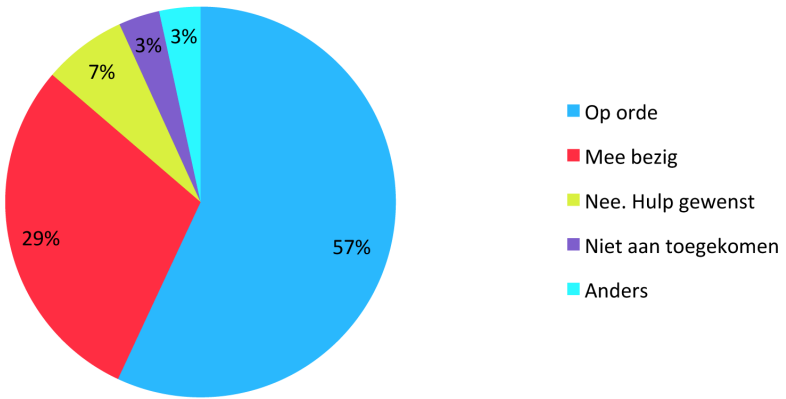
Benoem hier de maatregelen die u genomen heeft.

De meeste maatregelen die genoemd worden zijn voorlichting, opleiding en overleg. Daarnaast maatregelen als het vastleggen van verplichtingen voor medewerkers in de vorm van protocollen of instructies en gedragsregels als clean desk policy, het gebruik van shredders en regels voor het verzenden van e-mails.

Ook worden technische maatregelen genoemd zoals het aanscherpen van wachtwoordbeleid, het aanpassen van de software, het introduceren van portals, het beveiligen van data door antivirussoftware en versleuteling en het beperken van de toegang tot systemen.

11. Heeft u het idee dat u de beveiliging voor de verwerking van persoonsgegevens op orde heeft?

Uit de enquête blijkt dat 4 op de 10 respondenten hun beveiliging niet op orde hebben. Eén van de belangrijkste verplichtingen uit de AVG is dat bedrijven passende beveiligingsmaatregelen dienen te treffen t.b.v. een veilige omgang met persoonsgegevens. Passend wil zeggen dat rekening dient te worden gehouden met aard, omvang, context en doel van de verwerking en de ernst en waarschijnlijkheid van daaruit volgende risico's. Bij vraag 16 geven respondenten aan dat risico's voor de bedrijfsvoering als gevolg van de AVG zelfs zijn toegenomen. Positief is te zien dat de helft van de respondenten zegt dit jaar meer te zullen gaan investeren in technische beveiligingsmaatregelen (zie vraag 15).

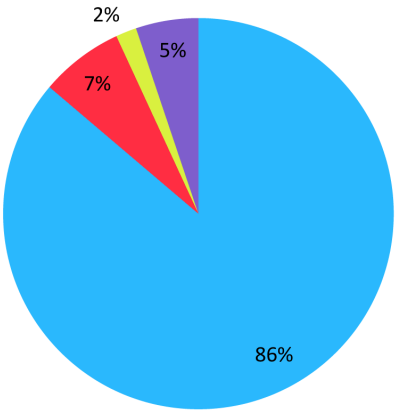


57%	Op orde
29%	Mee bezig
7%	Nee. Hulp gewenst
3%	Niet aan toegekomen
3%	Anders

12. Heeft u na mei 2018 al datalekken gemeld?

Een datalek is een - bedoelde of onbedoelde - inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Uit "*Overzicht feiten en cijfers 2018*" van de AP blijkt dat 26% van de datalekken plaats hebben gevonden in de financiële sector.



- Nee, wel incidenten maar geen privacyrisico's
- Nee, wel beveiligingsincidenten gehad maar geen privacyrisico's
- Ja, gemeld AP, melden aan betrokkene was niet nodig
- Ja, gemeld AP en aan betrokkenen

86%	Nee, wel beveiligingsincidenten gehad maar geen privacyrisico's
7%	Nee, geen datalekken of beveiligingsincidenten gehads
2%	Ja, gemeld AP, melden aan betrokkene was niet nodig
5%	Ja, gemeld AP en aan betrokkenen

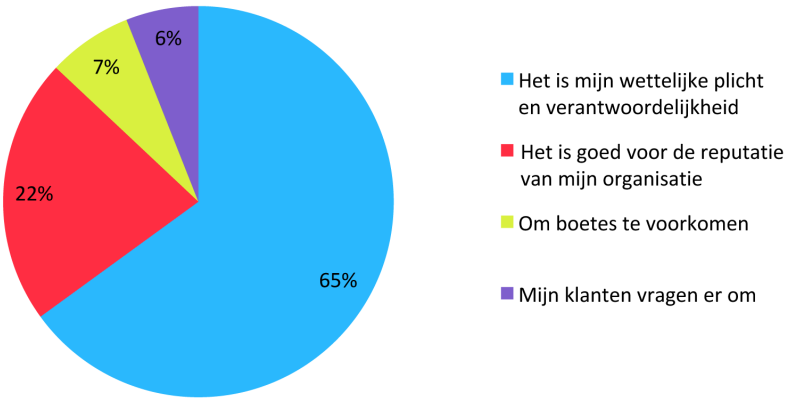
13. Weten uw medewerkers wat een datalek is en weten ze bij wie ze dat, als ze vermoeden dat er sprake van een datalek is, moeten melden?

De AVG stelt strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of u aan de meldplicht heeft voldaan.

De AVG vraagt erom dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van privacyregels.

14. Wat is voor uw organisatie de belangrijkste reden om de verwerking van persoonsgegevens en de privacy van uw klanten en medewerkers serieus te nemen?

De meeste noemen defensieve redenen om invoering van de AVG serieus te nemen namelijk het naleven van de wet en het voorkomen van boetes. Slechts in 3 van de 10 gevallen worden klanten en de reputatie van het bedrijf genoemd als driver om serieus met persoonsgegevens om te gaan.

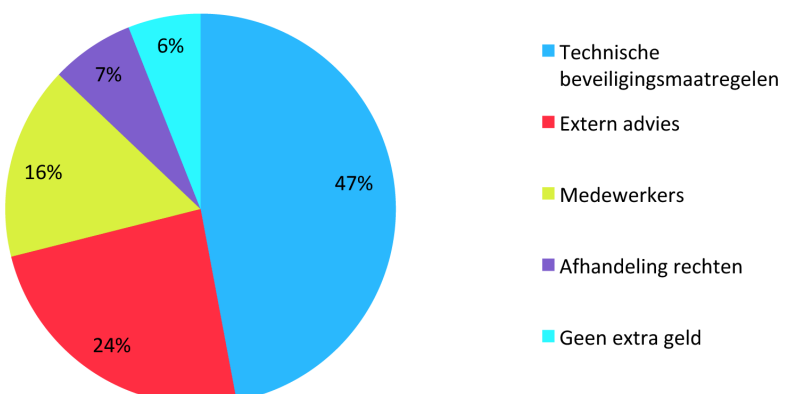


65 %	Het is mijn wettelijke plicht en verantwoordelijkheid
22 %	Het is goed voor de reputatie van mijn organisatie
7 %	Om boetes te voorkomen
6 %	Mijn klanten vragen er om

15. Voor welke posten verwacht u in 2019 meer geld te zullen besteden?

De AVG is er duidelijk over dat het niet voldoende is om eenmalig privacy beschermende maatregelen te treffen. Randvoorwaarden zoals bijvoorbeeld technische ontwikkelingen en regelgeving zijn voortdurend aan veranderingen onderhevig. De effectiviteit van genomen maatregelen dient dan ook met regelmaat te worden geëvalueerd en waar nodig aangepast.

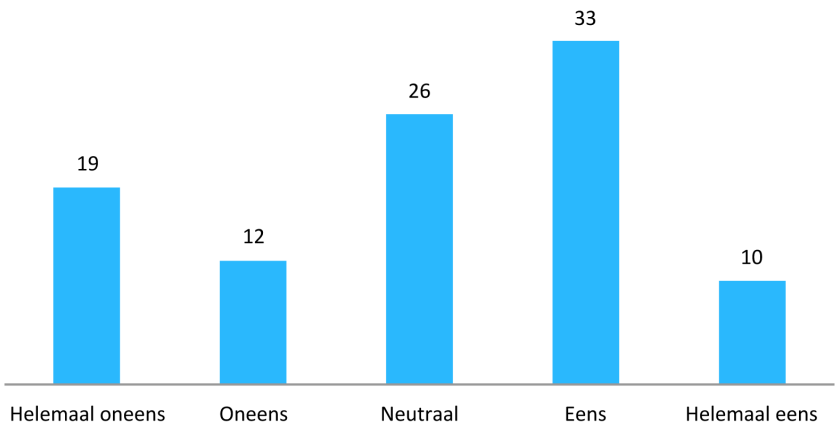
Als er geïnvesteerd wordt in maatregelen om persoonsgegevens conform de eisen van de AVG te verwerken dan is dat met name in technische beveiligingsmaatregelen en in maatregelen om medewerkers te trainen.
Om deze maatregelen mogelijk te maken verwacht een kwart van de respondenten daarvoor extern advies in te kopen.



47 %	Technische beveiliging-maatregelen
24 %	Extern advies
16 %	Medewerkers
7 %	Afhandeling rechten
6 %	Geen extra geld

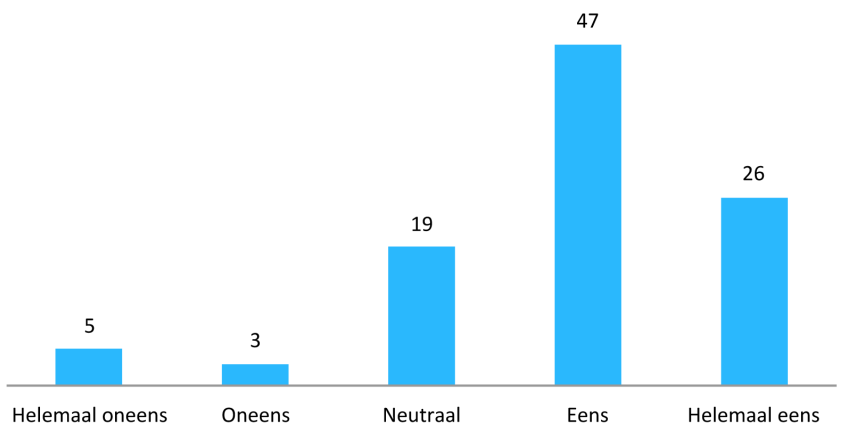
16. Stelling: Voor mijn organisatie zijn de bedrijfsrisico's met het in werking treden van de AVG toegenomen?

Eén van de kernthema's van AVG is accountability ook wel de verantwoordingsplicht genoemd. Als bedrijf moet je kunnen aantonen hoe er invulling is gegeven aan het nakomen van de AVG-verplichtingen. Datalekken zijn primair een risico voor betrokkenen maar in tweede instantie zeker ook een risico voor de organisatie en mogelijk zelfs voor de sector in de zin van imagoschade. Zo wordt het geven van boetes door privacytoezichthouders in Europa wordt veelal breed uitgemeten in de pers.



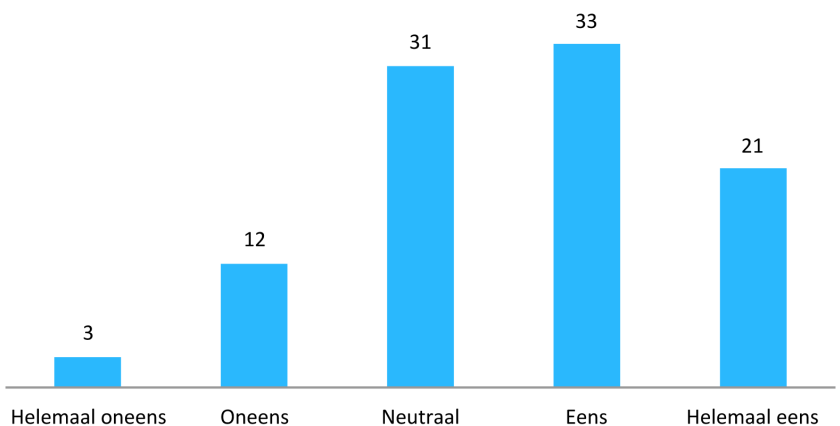
17. Stelling: Met de komst van de AVG is het privacy bewustzijn bij medewerkers van onze organisatie toegenomen.

Medewerkers vormen een belangrijke schakel in de beveiliging van privacygevoelige en vertrouwelijke informatie. Bewustwording op het gebied van privacy en de nieuwe wetgeving is dan ook een vereiste voor de hele organisatie. Medewerkers moeten kunnen inschatten wat de impact van de AVG is op processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Zogenaamde bewustwording programma's bevorderen het risicobesef en bewustwording van medewerkers en helpen bij het voorbereiden van de organisatie (zie ook vraag 10) Driekwart van de respondenten onderschrijft de stelling dat deze bewustzijn is toegenomen.



18. Stelling: We hebben overzicht van al onze verwerkers, en weten welke persoonsgegevens zij namens ons verwerken en hebben verwerkersovereenkomsten met ze afgesloten.

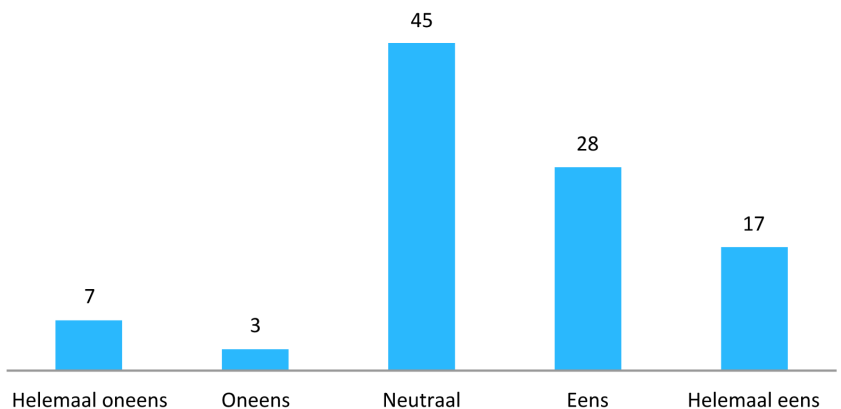
Een meerderheid is het (helemaal) eens met deze stelling en voldoet hiermee aan de wettelijke verplichting. Een groot deel is het echter niet eens met deze stelling en heeft niet met alle verwerkers een overeenkomst afgesloten.



19. Stelling: Mijn organisatie is in staat, als de Autoriteit Persoonsgegevens (AP) daar om vraagt, om met documenten aan te tonen dat de AVG wordt nageleefd.

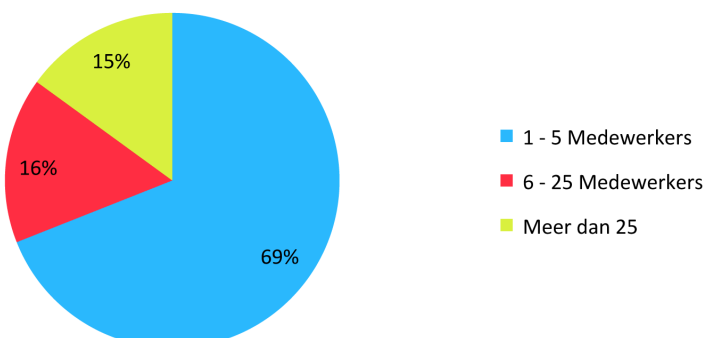
Het spreekt voor zich dat je de AVG naleeft, maar de AVG vraagt ook om deze naleving aan te tonen. Ook regelt de AVG dat je een verwerkingenregister op verzoek aan de Autoriteit Persoons-gegevens moet verstrekken. Hoe je dit aantoont is niet voorgeschreven.

Bijna de helft van respondenten geeft aan dit te kunnen aantonen, maar de meerderheid kan dit niet.



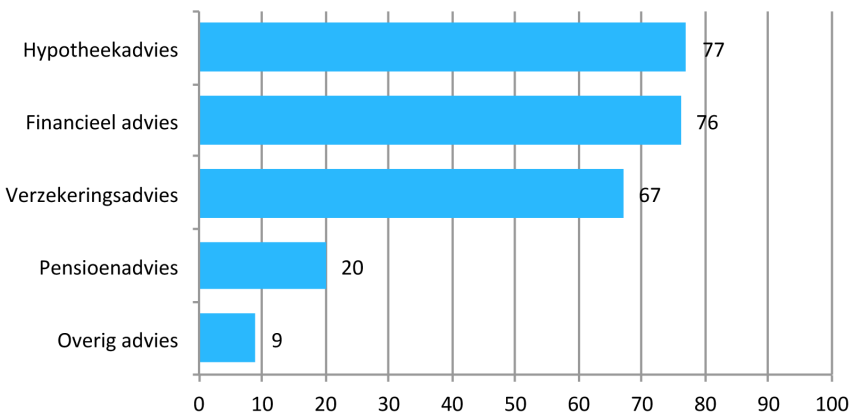
20. Hoeveel medewerkers heeft uw onderneming?

Zeven op de tien bedrijven hebben minder dan zes medewerkers in dienst. Bedrijven van deze omvang hebben vaak onvoldoende capaciteit om de AVG goed zelfstandig te implementeren. Implementatie komt dan ook vaak aan op de directeur zelf die ook de tijd moeilijk kan vinden. Ook zijn juist deze relatief kleinere bedrijven erg afhankelijk van grotere leveranciers en derden. Die afhankelijkheid vraagt om extra aandacht voor juiste processen en AVG-documentatie.



69%	1 - 5 medewerkers
16%	6 - 25 medewerkers
15%	Meer dan 25 medewerkers

21. In welke vormen van dienstverlening bent u actief?



DPO Network
Jan van den Berg
j.vandenberg@dponetwork.nl
+31 (0) 6 29 55 6314

Gerrit van Rooij
g.vanrooij@dponetwork.nl
+31 (0) 6 22 99 74 86

Volg ons op LINKEDIN
https://nl.linkedin.com/company/dpo-network

DPO Network

DPO Network is specialist op het gebied van Privacy Management in de automatisering en de financiële dienstverlening.

DPO Network
Diemermere 3
1112 TA Diemen

www.dponetwork.nl
+31 (0) 20 758 21 15