DE NATIONALE

PRIVACY BENCHMARK RETAIL 2020

ContaKT CONSULTING BV

Inhoudsopgave

Wat zijn de ervaringen van Retail Nederland?

De AVG is nu ruim twee jaar in werking. Voorafgaand aan 25 mei 2018, de datum dat de AVG in werking trad, maar ook daarna hebben veel organisaties tal van veranderingen in de bedrijfsvoering doorgevoerd. En veel organisaties zijn nog steeds bezig met implementatie van maatregelen om aan de AVG te voldoen.

De nationale Privacy Benchmark Retail, een initiatief van Contakt Consulting, onderzoekt de stand van zaken rondom de AVG in de retailsector. Wat zijn de ervaringen van Retail Nederland in het tweede jaar dat de AVG operationeel is? Is de implementatie volledig achter de rug of zijn er nog zaken die gerealiseerd moeten worden? Hoe verhouden deze vragen zich tot het eerste jaar dat de AVG in werking is getreden en wat zijn de ervaringen met het uitvoeren van de AVG? Deze en tal van andere vragen over de verschillende aspecten van de AVG komen in deze benchmark aan de orde en geven inzicht in de situatie van Retail Nederland.

Dit jaar wordt in de retail benchmark bijzondere aandacht gegeven aan de volgende vier onderwerpen:

- Privacy bewustzijn (awareness) op de winkelvloer
- Controle van verwerkers, hoe dan?
- Informatiebeveiliging van persoonsgegevens
- Certificering voor de AVG

We hopen dat de resultaten van dit onderzoek inspiratie geven om eventuele tekortkomingen in de toepassing van de AVG op te pakken. Tot slot willen we alle respondenten hartelijk bedanken voor hun bijdrage aan het onderzoek.

Ad Boumans
Douwe Douma
René van Eijk
Lodewijk Benjaminse
Ronald van Putten
Dick Sepers

Constateringen van het onderzoek

Er is meer inspanning nodig om te voldoen aan de AVG

Alhoewel er verbeteringen zijn gerealiseerd ten opzicht van de uitkomsten van de privacy benchmark van vorig jaar, blijkt uit het onderzoek dat op een aantal vlakken meer inspanning nodig is van retailers om te voldoen aan de verordening. Zo heeft 1 op de 10 retailers geen privacybeleid en onderhoudt 30% het verwerkingenregister niet. 31% van de respondenten beschikt niet over verwerkersovereenkomsten met alle verwerkers. Slechts 28% van de respondenten controleert alle verwerkers en slechts een klein deel van de verwerkers legt proactief verantwoording af. Hier ligt nog een grote uitdaging. Bij 27% van de respondenten ontbreekt een proces om persoonsgegevens conform de bewaartermijnen te verwijderen.

Datalekken vormen een financieel risico

77% van de respondenten registreert datalekken. 19% doet dat niet en loopt risico op forse boetes. Bij 15% ontbreekt een procedure datalekken. De meeste datalekken die bij retailers optreden, hebben betrekking op het versturen of afgeven van persoons-gegevens aan de verkeerde persoon. Bij 1 op de 8 respondenten (12%) is een hack-, malware- of phishingpoging succesvol geweest. 77% van de respondenten doet geen simulatieoefening van een groot datalek.

Privacybewustwording is geen eenmalige actie

Uit het onderzoek is gebleken dat er meer behoefte is aan privacybewustzijn bij leiding-gevenden en medewerkers. 31% van de respondenten geeft aan dat er periodiek aandacht is voor awareness in de vorm van een training of een e-learning. De meeste activiteiten hebben eenmalig plaatsgevonden.

Informatiebeveiliging verdient meer aandacht

Het waarborgen van privacy vereist de bescherming van persoonsgegevens. 69% van de retailers heeft een informatie-beveiligingsbeleid; 15% heeft dat niet.
In de AVG is een verplichting opgenomen om actief aan informatiebeveiliging te doen.
Het ontbreken van adequate informatie-beveiliging is een schending van de AVG en dus een belangrijk onderwerp. Bij 39% van de repondenten staat dit onderwerp regelmatig op de agenda van de directie.

Autoriteit Persoonsgegevens houdt toezicht en handhaaft

De rol van de Autoriteit Persoonsgegevens (hierna AP) verandert. In 2018 vervulde de AP meer de rol van vraagbaak, verstrekte uitleg over de AVG en gaf voorlichting aan brancheorganisaties. Dat is aan het veranderen in 2020. De AP richt zich meer op toezicht, handhaven en waar nodig beboeten. Eén op de zeven respondenten heeft inmiddels te maken gehad met de AP in de rol van toezichthouder.

Onvoldoende inzicht in de privacy risico's van (wijzigingen van) verwerkingen

Bij een nieuw project voert 31% van de respondenten een data protection impact assessments (DPIA) uit. 69% voert geen DPIA uit en is daardoor niet op de hoogte van privacyrisico's en zal daardoor niet afdoende maatregelen treffen.

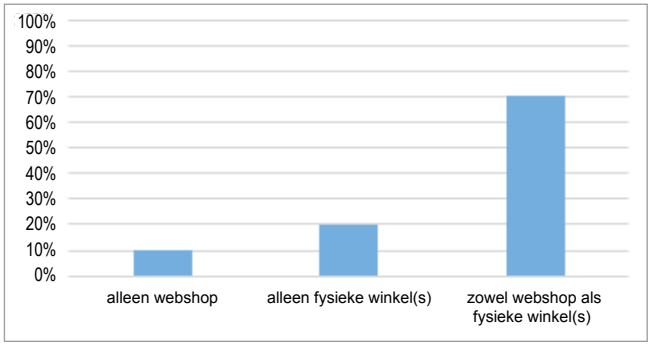
1. Nationale Privacy Benchmark Retail 2020

Dit rapport bevat de belangrijkste uitkomsten van de Nationale Privacy Benchmark Retail over 2020. Het onderzoek is gericht op retailorganisaties die zowel offline als online actief zijn

1.1 Wie deden er mee?

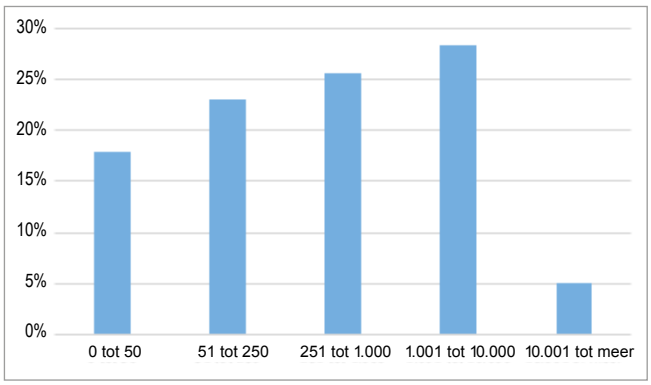
Respondenten vertegenwoordigen circa 11.000 winkeldeuren en 120.000 medewerkers. 70% van de deelnemende bedrijven heeft zowel webwinkels als fysieke winkels.

Deelnemende bedrijven



De deelnemende bedrijven verschillen qua aantallen medewerkers. Zwaartepunten liggen in de categorieën 250 tot 1.000 fte en 1.001 tot 10.000 fte.

Aantal medewerkers



1.2 Over de opzet van dit rapport

In het eerste deel van het rapport belichten we de stand van zaken met betrekking tot een aantal verplichtingen uit de AVG. In deel twee wordt stilgestaan bij de aandacht van de directie voor dit onderwerp, de aandacht vanuit de AP en andere partijen zoals de Consumentenbond. In deel drie wordt aandacht besteed aan informatiebeveiliging. Dit is nauw verbonden met privacy. Tot slot staan we in deel 4 stil bij certificeringen. Wanneer een organisatie een certificaat behaalt met betrekking tot informatiebeveiliging en/of privacy, toont het daarmee aan op deze terreinen afdoende maatregelen te hebben getroffen. Interessant om te weten hoe dat in de retailsector zit.

2. Is de retailsector AVG compliant?

De Algemene verordening gegevensbescherming (AVG) legt de verantwoordelijkheid bij organisaties zelf om aan te tonen dat aan de privacywet- en regelgeving wordt voldaan. Door te voldoen aan de verantwoordingsplicht (accountability) leveren organisaties een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

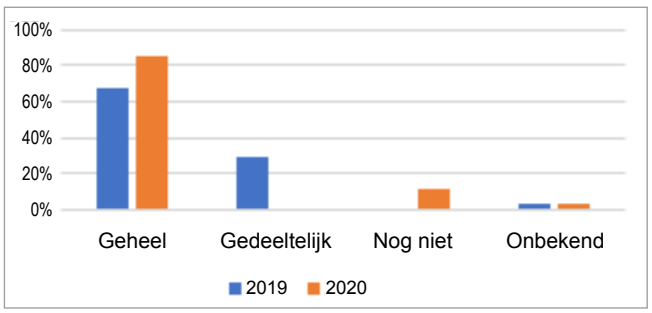
2.1 Verantwoordingsplicht

De AVG dwingt organisaties om goed na te denken over de verwerking en bescherming van persoonsgegevens. De verantwoordingsplicht houdt in dat organisaties moeten kunnen aantonen dat verwerking van persoonsgegevens aan de regels van de AVG voldoet, zoals rechtmatigheid, transparantie, doelbinding en juistheid. Daarnaast kent de AVG tal van andere verplichtingen voor de verwerkingsverantwoordelijke waarbij de bewijslast in een privacy-administratie moet worden vastgelegd. In dit hoofdstuk worden de resultaten van het onderzoek weergegeven per onderwerp.

2.2 Privacybeleid

85% van de respondenten geeft aan dat zij beschikt over een door de directie goedgekeurd privacybeleid. Bij 11% van de respondenten ontbreekt een privacybeleid. 4% van de respondenten weet niet of er een privacybeleid is. Dat is een aanmerkelijke verbetering ten opzichte van 2019, waarbij nog maar 68% van de respondenten aangaf te beschikken over een goedgekeurd privacybeleid en 29% aangaf geen privacybeleid te hebben of er nog mee bezig te zijn.

Privacy beleid



2.3 Privacyorganisatie

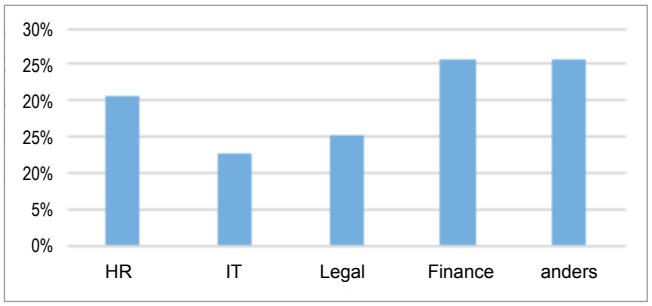
De AVG verplicht bepaalde categorieën organisaties om een Functionaris voor Gegevensbescherming (FG) aan te stellen. Een dergelijke functionaris houdt toezicht op naleving van de AVG binnen de organisatie. Voor retailorganisaties is deze aanstelling niet verplicht. Eén respondent heeft een FG aangesteld.

Een groot deel van de respondenten heeft de functie van Privacy Officer ingesteld. Een Privacy Officer is deskundig op het gebied van privacy en helpt de organisatie te voldoen aan de privacywetgeving.

Deelnemende retailorganisaties hebben de rol van Privacy Officer ondergebracht bij verschillende stafafdelingen zoals Finance, HR, Legal of IT. Een kwart van de respondenten geeft aan dat de rol elders binnen de organisatie is ondergebracht: marketing, secretariaat, een combinatie van secretariaat en ICT, controlling, kwaliteitsmanager of een externe professional.

In een enkel geval is nog niet bepaald welke medewerker de rol van Privacy Officer vervult. Kortom, de invulling van deze rol is zeer divers en bij de meeste organisaties gecombineerd met een andere functie.

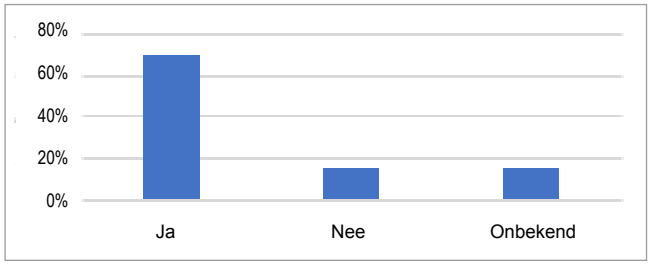
Privacy Officer combinatie met andere functie



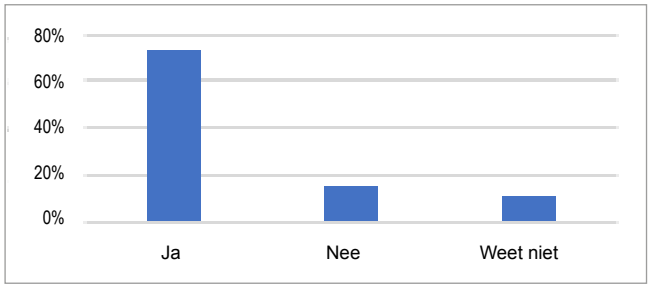
2.4 Privacy- en cookieverklaring

Een organisatie die persoonsgegevens verwerkt is verplicht haar klanten daarover te informeren (het recht op informatie zoals dat in de AVG wordt genoemd). Veel retailorganisaties gebruiken hiervoor de privacy- en cookieverklaring op de website. Bijna 70% van de respondenten geeft aan de privacyverklaring op de website regelmatig bij te werken en 73% geeft aan de cookieverklaring bij te werken.

Wordt de privacyverklaring op de website bijgewerkt?



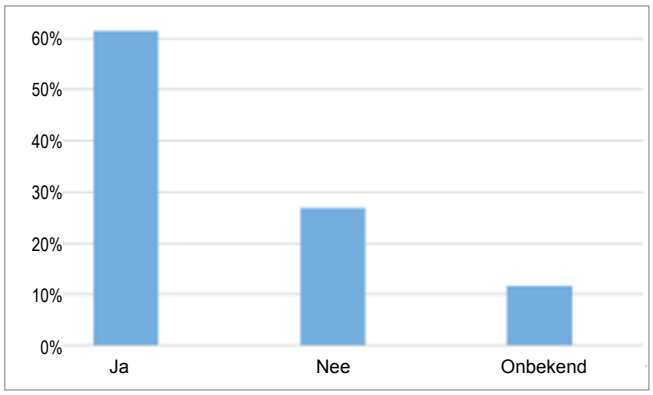
Wordt de cookieverklaring op de website bijgewerkt?



Voor de resterende organisaties ligt hier een opdracht; 30% van de respondenten heeft een privacyverklaring die niet is bijgewerkt of weet niet of deze wordt bijgewerkt en 27% heeft een niet bijgewerkte cookieverklaring. Verstrekt een organisatie onjuiste informatie aan betrokkenen, dan kan dat leiden tot klachten, negatieve publiciteit en, als het tegenzit, tot boetes.

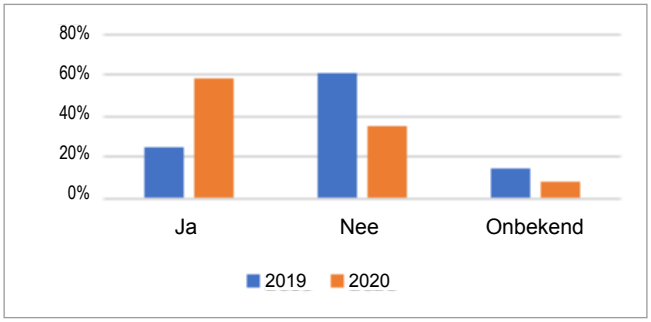
Ongeveer 61% van de respondenten geeft aan dat de cookieverklaring op de website voldoet aan de vereisten uit de AVG en de Telecommunicatiewet.

Voldoet cookieverklaring aan de eisen van AVG en Telecommunicatiewet?



De cookieverklaring is een verplichting vanuit de Telecommunicatiewet. Deze nationale wet wordt op termijn vervangen door de Europese e-Privacy verordening. Wanneer de e-Privacy verordening is ingevoerd, geldt deze direct in alle EU-lidstaten. 58% van de respondenten geeft aan op de hoogte te zijn van de inhoud van de e-Privacy verordening en te weten wat de impact is voor de organisatie. In 2019 was dat nog maar 25% van de organisaties. 35% van de respondenten weet niet wat de e-Privacyverordening inhoudt en wat de gevolgen kunnen zijn voor de eigen organisatie. Dat was in 2019 nog 60%. Dat betekent dat ten opzichte van de vorige enquête, een toenemend aantal van de respondenten de ontwikkelingen op dit terrein volgt en steeds beter op de hoogte lijkt te zijn. Desondanks weet 8% van de respondenten niet of er in de organisatie aandacht aan wordt besteed. Voor deze groep is er werk aan de winkel.

Kennis gevolgen e-privacyverordening



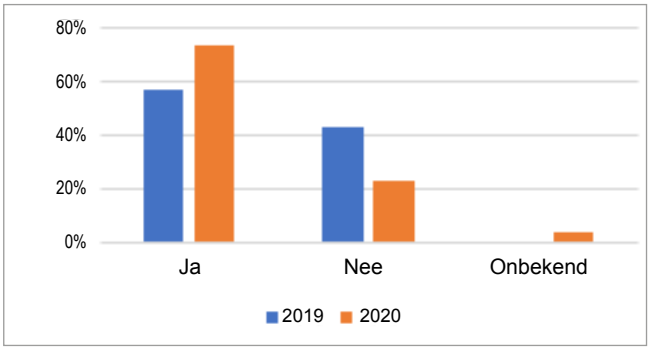
Cookie en e-Privacy verordening

De e-Privacy verordening is erop gericht elke EU-inwoner in vrijheid deel te laten nemen aan de digitale maatschappij. Een cookiewall belemmert dat uitgangspunt en is verboden. Tracking cookies die het internetgedrag volgen over websites ondermijnen de vrije deelname en zijn verboden als er geen expliciete toestemming is. En als de toestemming niet wordt gegeven moet de website wel toegankelijk blijven.

2.5 Register van verwerkingen

De AVG vereist dat elke organisatie die persoonsgegevens verwerkt, overzicht en inzicht heeft in wat het doet met persoonsgegevens. Concreet wordt door de AVG voorgeschreven dat er een verwerkingenregister moet worden bijgehouden. 73% van de respondenten geeft aan dit register daadwerkelijk te onderhouden, waar dat in 2019 nog maar 57% was. 27% van de respondenten doet dat niet, tegen 42% in 2019. Dus steeds meer retailorganisaties ondernemen actie ten aanzien van het verwerkingenregister. Het is belangrijk het verwerkingenregister bij te houden, omdat het onder andere de organisatie zélf handig inzicht geeft in de persoonsgegevens die de organisatie verwerkt, met welk doel, op basis van welke rechtsgronden en met wie de persoonsgegevens worden gedeeld. Veel retailorganisaties hebben wel een verwerkingenregister opgebouwd, maar wanneer dit register niet wordt onderhouden, kan men niet vertrouwen op de informatie in dat register. Daarmee zijn de inspanningen om het register op te bouwen te beschouwen als verloren moeite. Daarnaast is de vraag of een organisatie in dat geval een volledig beeld heeft van haar verwerkingen met persoonsgegevens en of een juiste en complete weergave kan worden gegeven bij een inzageverzoek van een betrokkene.

Onderhouden verwerkingsregister



Het nut van het verwerkingenregister

In het verwerkingenregister houdt een organisatie bij in welk land persoonsgegevens worden verwerkt. Deze informatie is behulpzaam bij het bepalen van de consequenties van de recente uitspraak van het Europese Hof. Het Hof heeft in juli 2020 het Privacy Shield ongeldig verklaard, waardoor de verwerking van persoonsgegevens in de Verenigde Staten op basis van het Privacy Shield, in feite niet meer is toegestaan. Inzicht in de locaties waar persoonsgegevens worden verwerkt, helpt bij het onderzoeken van de consequenties van deze uitspraak. Het verwerken van persoonsgegevens buiten de EU kan ook door een subverwerker plaatsvinden. Dit maakt het noodzakelijk dat er inzicht is in de gehele keten van gegevensverwerking.

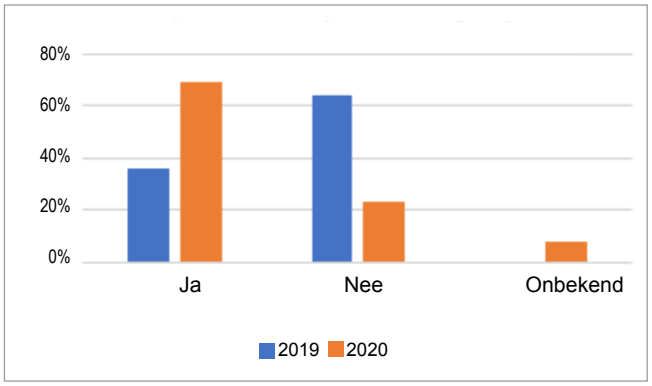
2.6 Verwerkersovereenkomsten

Het uitbesteden van verwerkingen van persoonsgegevens aan een dienstverlener, een verwerker in AVG termen, wordt veelal geregeld in een verwerkersovereenkomst. In 2019 gaf 36% van de respondenten aan dat er verwerkersovereenkomsten zijn afgesloten en dit jaar geeft 69% van de respondenten aan dat er dergelijke overeenkomsten zijn. Een enorme vooruitgang maar het betekent ook dat nu, twee jaar na inwerkingtreding van de AVG, 31% van de respondenten aangeeft hier nog niet klaar mee te zijn. Daarmee wordt door deze organisaties niet voldaan aan de eis van de AVG om voor elke uitbesteding een verwerkersovereenkomst af te sluiten. Los van de wettelijke verplichting ontbreken

er dan ook afspraken tussen de organisatie en de dienstverlener over het opvolgen van rechten van betrokkenen, datalekken, audits, aansprakelijkheid, etc. Daarmee lopen deze organisaties de volgende risico's:

- boete door de AP want er is niet voldaan aan de AVG;
- conflicten met de verwerker omdat er geen heldere afspraken zijn vastgelegd en verdere escalatie op het moment dat het fout gaat.

Verwerkingsovereenkomsten afgesloten

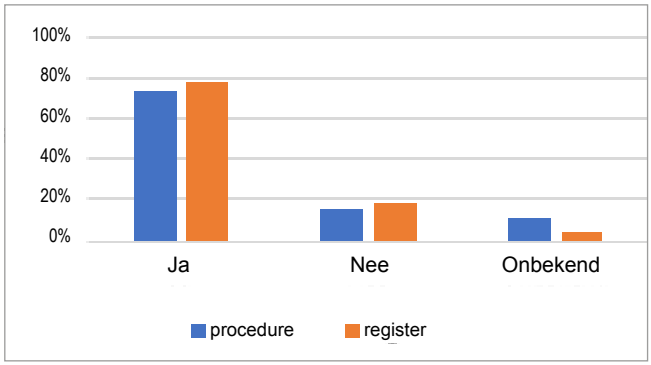


2.7 Procedure datalekken

Een kleine 75% van de respondenten geeft aan te beschikken over een procedure om datalekken tijdig af te handelen; dit komt in grote lijnen overeen met de situatie in 2019. Door een procedure in te richten, geeft een organisatie aan klaar te zijn om een datalek af te kunnen handelen. Een vervolgstap is deze procedure periodiek te oefenen, zodat medewerkers die betrokken zijn bij de opvolging van het datalek, weten hoe ze moeten handelen als een grootschalig datalek optreedt. Vergelijk dit met een brand- of ontruimingsoefening, wat al heel gebruikelijk is bij vele organisaties. 25% van de respondenten geeft aan niet voorbereid te zijn op een datalek. Zij lopen een risico als het gaat om het tijdig melden van een datalek. De boete bij het niet of te laat melden ligt tussen €300.000,- en €750.000,-.

Onderdeel van de registratieplicht van de AVG is de vastlegging van incidenten in een datalekregister. Hierin dienen alle beveiligingsincidenten te worden vastgelegd met relevante informatie over het datalek, waaronder de gemaakte afweging voor wel of niet melden van het datalek aan de AP en eventueel de betrokkenen.

Datalekken afgehandeld

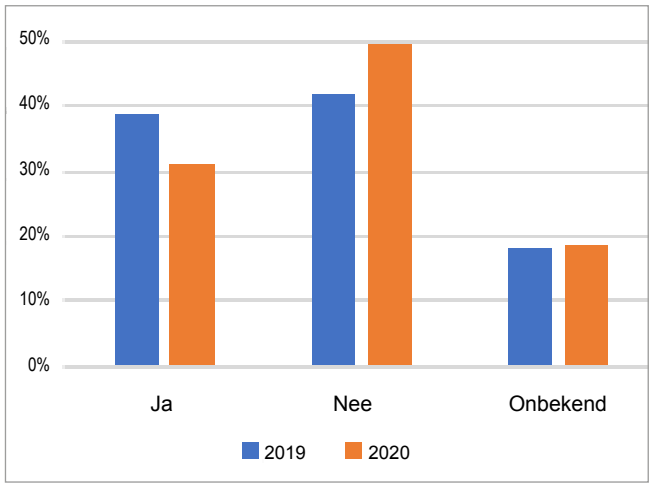


2.8 DPIA

Een Data Protection Impact Analysis (DPIA) is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en op basis daarvan te bepalen welke maatregelen genomen moeten worden om de risico's te verkleinen. De AVG verplicht organisaties om een dergelijke analyse uit te voeren wanneer de gegevensverwerking waarschijnlijk een hoog risico oplevert voor de mensen van wie de organisatie de persoonsgegevens verwerkt. De DPIA dient te worden uitgevoerd bij een nieuwe verwerking, een nieuw systeem of bij ingrijpende aanpassingen van bestaande verwerkingen of systemen. Slechts 31% van de respondenten geeft aan DPIA's uit te voeren. Daar ligt dus nog een uitdaging voor ongeveer 70% van de respondenten om dit proces op orde te krijgen.

Een mogelijke oorzaak van het feit dat maar weinig organisaties DPIA's uitvoeren, is wellicht onwetendheid of onbekendheid met de inhoud van een DPIA. Een Privacy Officer is op de hoogte van deze eis uit de AVG en kan zijn kennis inbrengen, maar slechts 50% van de respondenten geeft aan de Privacy Officer daadwerkelijk te betrekken bij implementatie- of veranderprojecten.

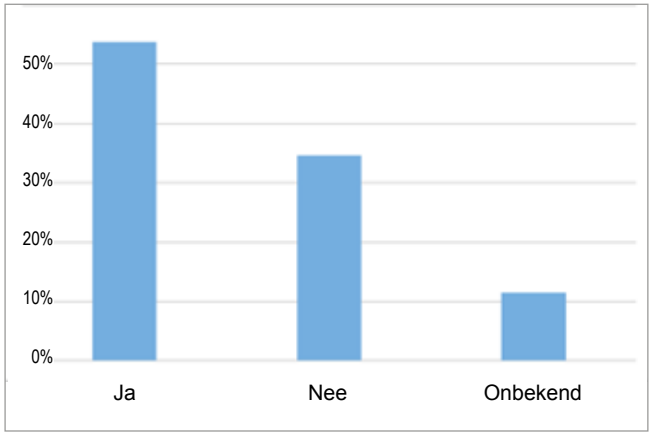
DPIA procedure uitgevoerd?



2.9 Verplicht DPIA

Bij een aantal verwerkingen verplicht de AP dat er een DPIA (Data Protection Impact Assessment) wordt uitgevoerd. Dat is bijvoorbeeld het geval bij cameratoezicht, het gebruik van een zwarte lijst, fraudebestrijding en controle van werknemers (bijvoorbeeld GPS-systemen in (vracht)auto's en controle van e-mail-en internetgebruik). Slechts 54% van de respondenten geeft aan deze verplichte DPIA te hebben uitgevoerd. Dat betekent dat 46% nog een inhaalslag heeft te maken.

Verplichte DPIA uitgevoerd?



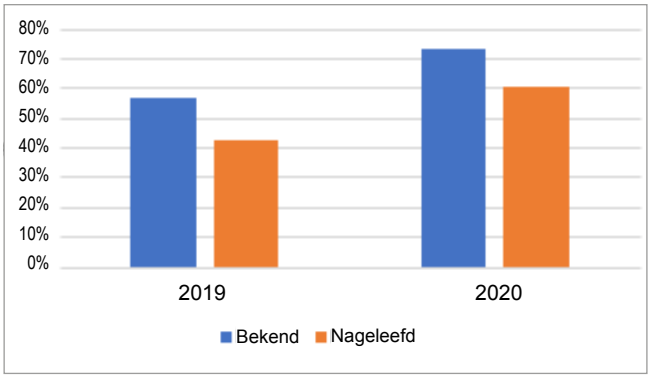
2.10 Bewaartermijnen

Wanneer persoonsgegevens niet meer nodig zijn voor het doel waarvoor ze zijn verzameld, moet een organisatie deze persoonsgegevens verwijderen. Hierbij moet een organisatie rekening houden met wettelijke bewaartermijnen.

73% van de respondenten geeft aan dat de bewaartermijnen van persoonsgegevens zijn vastgesteld en bekend zijn bij de verantwoordelijken binnen de organisatie. Dat is een toename ten opzichte van 2019 maar betekent nog wel dat bij 27% van de respondenten een kennisachterstand is. 61% geeft aan dat persoonsgegevens na de bewaartermijn ook daadwerkelijk worden verwijderd. Dat is iets meer dan in 2019, toen dat 43% was. Ook hier geldt dat nog steeds een behoorlijk percentage een inhaalslag heeft te maken.

50% van de respondenten kan aantonen dat de persoonsgegevens ook daadwerkelijk zijn verwijderd. Ook dat betekent voor de overige organisaties een inhaalslag. Immers de aantoonbaarheid is een verplichting die de AVG oplegt aan organisaties.

Bewaartermijnen bekend cq nageleefd



2.11 Aantal en aard van de datalekken

Een datalek is een beveiligingsincident waarbij persoonsgegevens per ongeluk of op onrechtmatige wijze verloren zijn gegaan, zijn vernietigd, zijn gewijzigd of waarbij persoonsgegevens zijn ingezien door onbevoegden. 44% van de respondenten geeft aan dat er in 2019 bij hen geen datalek is opgetreden. Het aantal datalekken is over het algemeen vrij gering waarbij het opvalt dat bij 4% van de respondenten er meer dan 51 datalekken zijn opgetreden. Gemiddeld elke week wel een datalek.

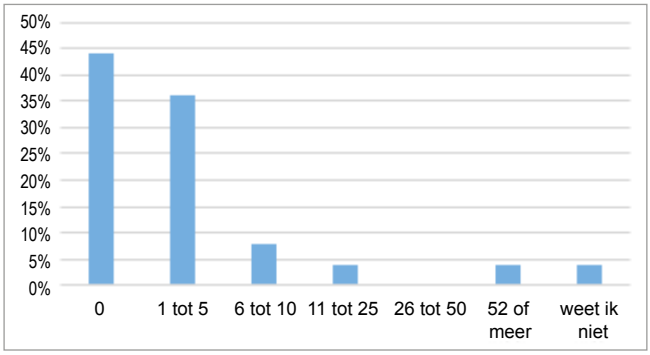
Het antwoord 'Geen datalek' kan twee dingen betekenen. Er is daadwerkelijk geen datalek geweest of er is wel een datalek geweest, maar dat is door niemand opgemerkt. 64% van de respondenten is van mening dat de medewerkers van de organisatie voldoende in staat zijn datalekken en beveiligingsincidenten te herkennen en te melden. Dat betekent voor 36% van de respondenten dat er op terrein van awareness nog werk aan de winkel is. Belangrijk werk omdat het niet of te laat melden een boete van de AP kan betekenen.

56% van het aantal opgetreden datalekken is niet gemeld aan de AP. Dat betekent dat de retailorganisaties bij die categorie datalekken hebben ingeschat dat er geen risico's waren voor de persoon/personen over wie gegevens zijn gelekt. 28% van het aantal datalekken is gemeld aan zowel de AP als aan de betrokken personen zelf. Dat betekent dat de betreffende retailorganisaties hebben ingeschat dat de datalekken grote risico's met zich mee kunnen brengen voor die personen. 12% van het aantal datalekken is alleen gemeld aan de AP. Deze percentages komen redelijk overeen met de percentages van 2019. Dat betekent dat er aan de ernst van de datalekken weinig is veranderd.

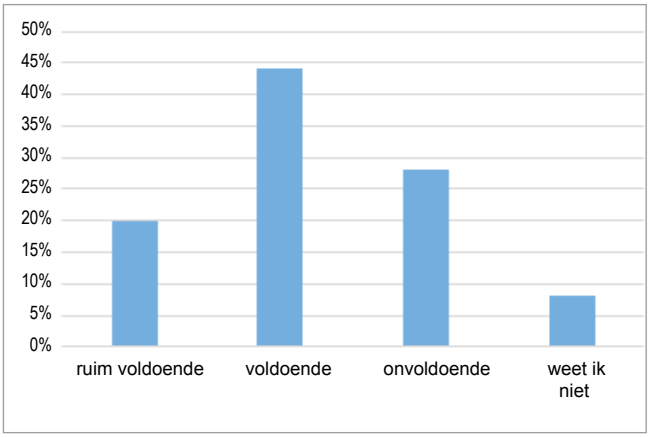
De aard van de datalekken is divers, maar de meeste datalekken worden veroorzaakt door

menselijk handelen, zoals het versturen van gegevens aan de verkeerde ontvanger, een geopende brief retour ontvangen of het verliezen van apparatuur met daarop persoonsgegevens. 12% van het aantal datalekken is veroorzaakt door hacking, malware, phishing en dergelijke activiteiten. Dit laatste betreft weliswaar een relatief gering aantal datalekken, maar meestal is de impact des te groter. Bij een verkeerd verzonden brief / e-mail betreft het vaak één persoon, maar bij een hackaanval kan het complete klantenbestand gestolen worden. Daarnaast kunnen de kosten flink oplopen als er ook ICT-forensisch onderzoek uitgevoerd moet worden om te bepalen waar de hacker toegang toe had en welke gegevens er zijn buitgemaakt.

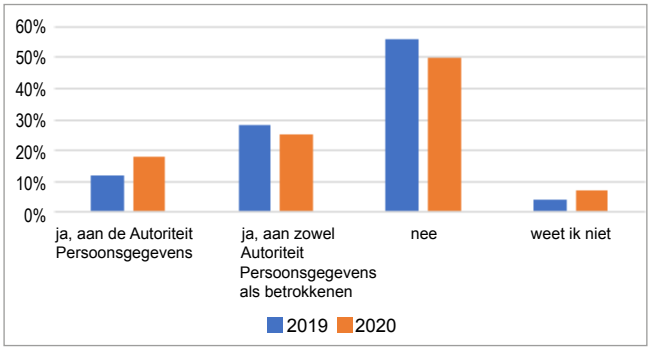
Aantal datalekken opgetreden



Datalekken herkennen en melden



Datalekken gemeld



	Response Percent
Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger	40%
Brief of postpakket kwijtgeraakt of geopend retour ontvangen	8%
Apparaat, gegevensdrager (bv. USB-stick) en/of papier kwijtgeraakt of gestolen	12%
Hacking, malware, phishing, CEO-fraude	12%
Persoonsgegevens per ongeluk gepubliceerd	8%
Persoonsgegevens van verkeerde klant getoond in portal	20%
Niet van toepassing	48%
Anders, namelijk	80%

2.12 Awareness

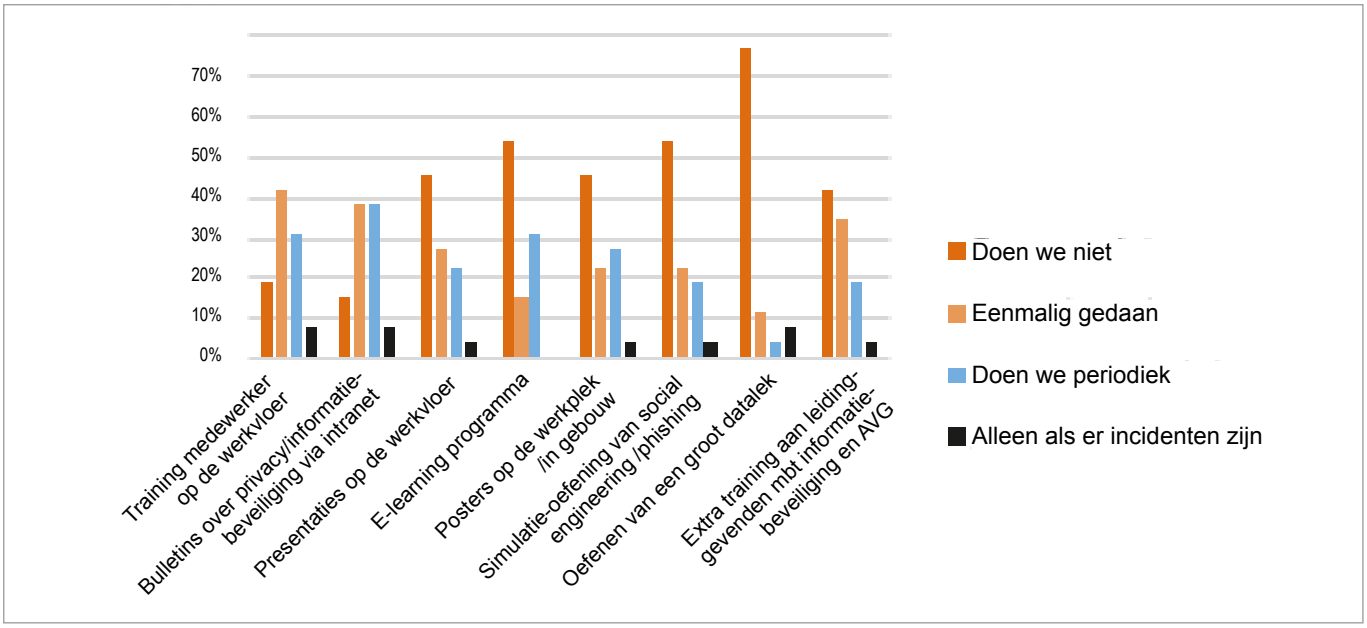
De mens is nog steeds de grootste veroorzaker van datalekken zoals hiervoor in paragraaf 2.11 beschreven. Periodieke aandacht voor privacy en informatiebeveiliging blijft daarom nodig. Enerzijds om mensen te overtuigen van het belang van informatiebeveiliging en privacy en anderzijds om alertheid ten aanzien van bedreigingen te verhogen. Awareness-sessies hebben ertoe geleid dat een groot deel van de respondenten van mening is dat medewerkers datalekken kunnen herkennen (zie hiervoor bij paragraaf 2.11). Maar kennelijk hebben deze sessies er nog niet toe geleid dat medewerkers zorgvuldiger omgaan met persoons-gegevens want de meeste datalekken komen voort uit menselijk handelen.

"Een aantal ah.nl-accounts is 16 oktober toegankelijk geweest voor andere klanten. Dat was een gevolg van werkzaamheden aan het systeem, zegt een woordvoerster van Albert Heijn. Er zijn volgens de woordvoerster geen meldingen binnengekomen van klanten die aangeven dat er ongewenste toegang tot hun account is geweest. Wel kreeg de supermarktketen een melding van een klant die de gegevens van een andere klant kon inzien. "We hebben de desbetreffende klant geïnformeerd dat het probleem direct is opgelost."

Albert Heijn heeft klanten gewaarschuwd alert te zijn op vormen van spam en phishing. "Wij onderzoeken dit voorval uitvoerig en treffen maatregelen om herhalingen te voorkomen. "De Autoriteit Persoonsgegevens is van het datalek op de hoogte gesteld."

Link/bron: https://retailtrends.nl/news/62217/datalek-bij-albert-heijn-door-werkzaamheden

Toegepaste methoden van Privacy awareness



Zorgvuldig omgaan met persoonsgegevens is essentieel om het aantal incidenten met persoons-gegevens te verlagen. Om aandacht te besteden aan dit onderwerp worden verschillende middelen ingezet: van e-learnings en training op de werkvloer tot posters aan de muur. Veelal eenmalig, soms periodiek.

Onderstaande tabel geeft aan welke maatregelen bij de respondenten worden getroffen voor de verbetering van de privacy awareness.

Herkennen van bedreigingen (zoals phishing en CEO-fraude) door medewerkers en leidinggevenden	54%
Privacy bewustzijn bij leidinggevenden	69%
Bewustzijn m.b.t. informatiebeveiliging bij medewerkers en/of leidinggevenden	69%
(H)erkennen van risico's door management	54%
Opstellen van richtlijnen over het gebruik van bedrijfsmiddelen (wachtwoorden, wifi, externe netwerken, eigen apparatuur)	27%
Uitdragen van richtlijnen (regels) aan medewerkers op het gebied van privacy en informatiebeveiliging en zorgen voor de naleving	46%
Weet ik niet	8%
Andere?	8%

Er is een diversiteit aan methoden om privacy awareness te versterken in de organisatie. Opvallend is dat niet regelmatig aandacht aan dit onderwerp geven relatief laag scoort.

Retailorganisaties geven aan extra maatregelen te willen nemen voor het versterken van awareness bij medewerkers en leidinggevenden

De verbeteringen richten zich op het vergroten van het privacybewustzijn én informatiebeveiligings-bewustzijn. Daarbij geeft 54% van de respondenten aan meer aandacht te willen besteden aan praktische onderwerpen zoals het herkennen van phishing mails en CEO-fraude. 46% van de respondenten geeft aan de richtlijnen (regels) op het gebied van privacy en informatiebeveiliging meer te willen uitdragen aan medewerkers. Kennelijk zijn de richtlijnen er wel, maar deze zijn onvoldoende uitgedragen naar medewerkers.

Waarom privacy bewustwording niet werkt

Veel bedrijven en organisaties kampen met hetzelfde probleem: het lukt niet om gedragsverandering bij medewerkers te realiseren als het gaat om het omgaan met persoonsgegevens. Zo worden bestanden met gevoelige persoonsgegevens bijvoorbeeld nog steeds onbeveiligd via e-mail gedeeld en blijft gevoelige informatie nog lang in de mailbox bewaard.

De grootste oorzaak van het mislukken van privacy bewustwording ligt in de aandacht die eraan gegeven wordt. Veelal zien we een eenmalige algemene presentatie over de privacywetgeving (AVG), aangevuld met wat artikelen op intranet. Op zich is uitleg over de AVG een goed begin, maar medewerkers zijn vooral geïnteresseerd in de toepassing in de dagelijkse praktijk; wat betekent de AVG voor mij en mijn afdeling? Immers, de omgang met persoonsgegevens is voor een klantenservice medewerker toch echt anders dan voor een HR-medewerker. Een one-size-fits-all aanpak resulteert niet in het gewenste resultaat. Hoe dan wel?

Tip 1: Combineer privacy en informatiebeveiliging

Voor nieuw gedrag is een lange adem nodig, waarbij gerichte aandacht nodig is voor het onderwerp en wat het bedrijf wil bereiken. Voor privacy geldt dit bij voorkeur in combinatie met informatie-beveiliging te doen. Want privacy en informatiebeveiliging kunnen niet los van elkaar worden gezien.

Tip 2: Zet een programma op

Periodiek aandacht besteden kan op verschillende manieren: trainingen, presentaties, teamoverleg, e-learning, phishing mail test, maar ook informatie op intranet en nieuwsartikelen. Dat is allemaal vorm. Belangrijker hierbij is dat de activiteiten zijn afgestemd op de doelgroep, zichtbaar zijn en periodiek worden uitgevoerd. Zet daarom een programma op, gericht op gedragsverandering. Door drukke agenda's van medewerkers is het een strijd om aandacht. Er moet dus goed nagedacht worden over (de boodschap voor) de doelgroep, de frequentie en het medium om te voorkomen dat de boodschap wegzakt in de dagelijkse drukte van medewerkers.

Tip 3: Bied ondersteuning

Als je gewoontes van mensen wilt veranderen, zul je ze daarbij moeten helpen. In plaats van te hameren op het gebruik van lange wachtwoorden, kan een password manager of single-sign-on als oplossing geboden worden. Bij gebruik hiervan kun je mensen er wel op attenderen dat dat ene wachtwoord heel belangrijk is.

Tip4 : Belonen

Om medewerkers te laten ervaren hoe gemakkelijk het is om op een phishing mail te klikken, kan een phishing test uitgevoerd worden. Ervaring is nog altijd de beste leermeester. Hierbij verzendt de organisatie zelf een phishing mail aan de medewerkers. Trapt er dan toch iemand in een phishing mail, dan kan de neiging ontstaan om die persoon erop aan te spreken. Daarmee wordt feitelijk een bom gelegd onder het hele bewustwordingsprogramma. Want als er iets is wat je niet wilt, dan is het dat mensen beveiligingsincidenten of onveilige situaties niet meer melden. Het melden is een voorwaarde om je als organisatie te kunnen verbeteren. Je kunt dit niet vaak genoeg benadrukken. Beloon medewerkers dus voor het melden. Een compliment of positieve aandacht doet wonderen.

Tip 5: Aantrekkelijk

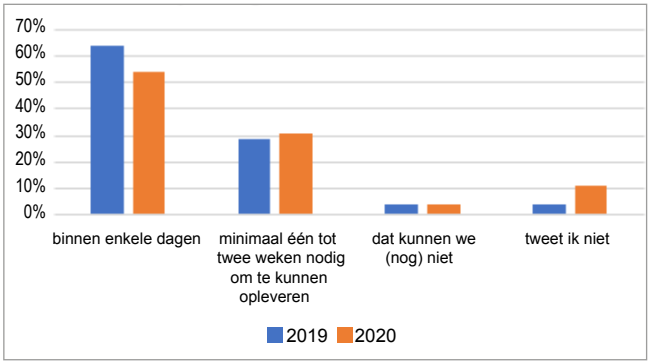
Tot slot is het de kunst om medewerkers niet te overladen met het onderwerp. Als je dit wel doet, dan creëert dit weerstand. In het bewustwordingsprogramma dien je hier dus rekening mee te houden. Dan blijft de boodschap aantrekkelijk en vergroot je de kans op succes.

2.13 Verantwoording

Het vereist nogal wat van een automobilist om aan te kunnen tonen dat alle keren dat hij/zij in de bebouwde kom reed, er werd voldaan aan de snelheidslimiet. Iets dergelijks is voor wat betreft de AVG wel op organisaties van toepassing. Een organisatie moet kunnen aantonen dat aan de AVG wordt voldaan, een zogenaamde omgekeerde bewijslast. Dit vereist een privacy administratie, gesteund met goede processen waaruit de verantwoording met onweerlegbaar bewijs blijkt. Daarnaast dienen (beveiligings)maatregelen te worden geëvalueerd en indien nodig geactualiseerd.

Op de vraag binnen welke termijn er gereageerd kan worden op een vraag van de AP om de privacy administratie op te leveren, antwoordt 54% van de respondenten binnen enkele dagen de gevraagde informatie te kunnen leveren. Kennelijk hebben deze respondenten de administratie op orde. 31% van de respondenten geeft aan enkele weken nodig te hebben. Dat betekent dat er wel een privacy-administratie is, maar dat deze nog niet geschikt is om te delen met AP. 4% geeft aan nog niet te kunnen voldoen aan de vraag van de AP en 11% weet niet of zijn/haar organisatie hiertoe in staat is. Dat betekent voor 15% van de respondenten dat zij niet voldoen aan de AVG. Gezien het feit dat 1 op de 7 respondenten inmiddels is benaderd door de AP, lopen de organisaties die geen informatie kunnen verstrekken een behoorlijk risico.

Tijd nodig om AP te antwoorden



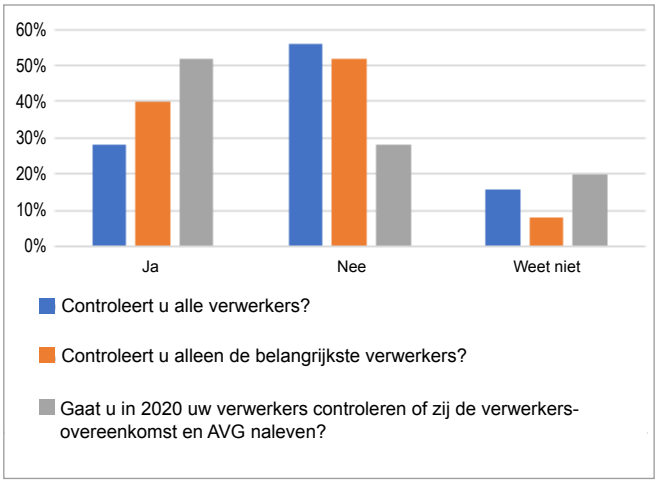
Overigens komen deze cijfers redelijk overeen met de situatie in 2019. Dat betekent dat de retail-organisaties nog volop verbeteringen kunnen, en in feite moeten, doorvoeren. Het feit dat het een aantal weken vergt voordat de AP kan worden beantwoord, kan worden opgevat als een signaal dat de privacy-administratie niet op orde is

2.13.1 Verantwoording door verwerkers

Om verantwoording te kunnen afleggen is ook informatie nodig van verwerkers. 28% van de respondenten geeft aan alle verwerkers te controleren, 40% geeft aan alleen de belangrijkste verwerkers te controleren en 52% heeft het voornemen om in 2020 verwerkers te controleren.

Al met al is hier een behoorlijke verbetering mogelijk en zelfs ook noodzakelijk. Alleen als een organisatie aantoonbaar kan maken dat een verwerker voldoet aan de AVG, kan daarover verantwoording worden afgelegd. In het privacybeleid wordt idealiter opgenomen op welke wijze de organisatie verantwoording aflegt.

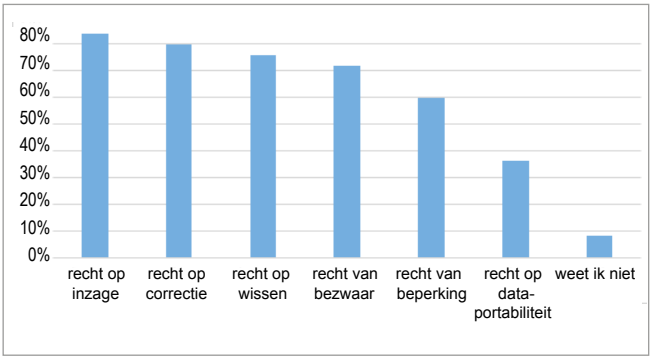
Controleren verwerkers



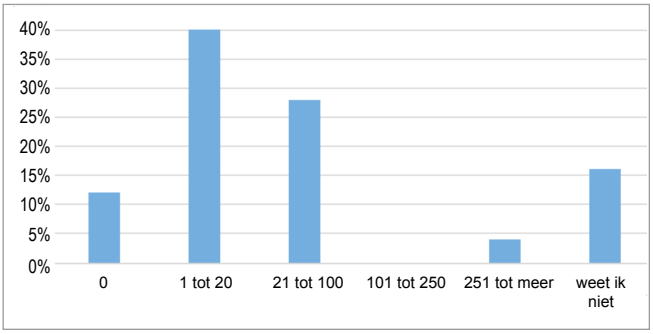
2.14 Rechten betrokkenen

Uit het onderzoek blijkt dat klanten en medewerkers van retailorganisaties in de meeste gevallen gebruik kunnen maken van alle rechten van betrokkenen die in de AVG worden genoemd. Van het recht op dataportabiliteit kan slechts bij 8% van de respondenten invulling geven. In de praktijk blijkt dit recht minder relevant voor betrokkenen en medewerkers in de retailbranche. Uit de grafiek kan verder afgeleid worden dat nog niet alle respondenten aan een beroep op de privacyrechten kunnen voldoen. Toch is dit een belangrijk onderdeel van een gezond privacybeleid. En een gezond privacybeleid draagt bij aan het vertrouwen van klanten en medewerkers in uw organisatie.

Rechten betrokkenen



Hoeveel verzoeken ontvangen?

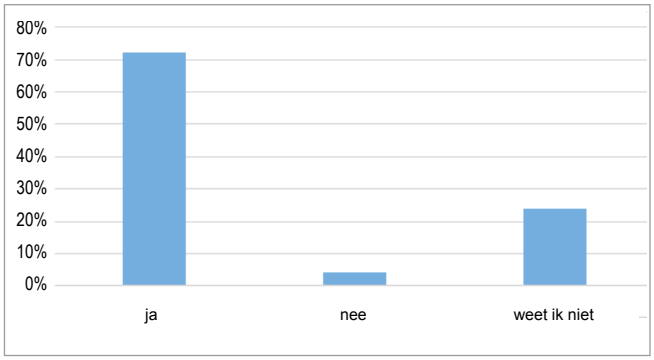


2.14.1 In hoeverre maken klanten en medewerkers nu gebruik van hun rechten onder de AVG?

We zien dat 80% van de respondenten geen tot minder dan 100 klantverzoeken op het uitvoeren van privacyrechten hebben ontvangen. 4% heeft meer dan 250 verzoeken ontvangen. 72% van de respondenten heeft klantverzoeken binnen de wettelijke termijn van één maand kunnen afhandelen. Bij 4% is dat niet gelukt en 24% van de respondenten geeft aan niet te weten of het gelukt is dergelijke verzoeken binnen de gestelde termijn af te handelen.

Onderdeel van de verantwoordingsplicht is dat een organisatie moet kunnen bewijzen dat rechten van betrokkenen tijdig en correct zijn opgevolgd. De verantwoording kan worden vastgelegd in een klantrechtenregister, waarbij datum ontvangst en datum afhandeling van het verzoek twee elementen zijn die hierin minimaal opgenomen dienen te worden.

Hoeveel verzoeken afgehandeld?



2.15 Overall resultaat

Uit de resultaten van het onderzoek kan worden geconcludeerd dat retailers sinds ons vorige onderzoek in 2019 niet hebben stilgezeten als het gaat om het voldoen aan de AVG. Zo zijn er meer respondenten die aangeven dat er een privacybeleid is (2019: 68%, 2020: 85%) en dat het verwerkingenregister wordt onderhouden (2019: 57%, 2020: 73%). Verder zijn er meer verwerkersovereenkomsten afgesloten (2019: 36%, 2020: 69%).

Toch is er ruimte voor verbetering op een aantal vlakken. Zo registreert 19% van de respondenten geen datalekken en wordt bij 50% van de respondenten geen DPIA uitgevoerd bij nieuwe verwerkingen of nieuwe systemen. Bij 27% van de respondenten ontbreekt een proces om persoonsgegevens te verwijderen als de bewaartermijn is versteken. 15% van de respondenten geeft aan geen informatiebeveiligingsbeleid te hebben. Ook als het gaat om het toetsen van beveiligingsmaatregelen en verwerkers is er nog verbetering mogelijk. Het uitvoeren van verbeteringen op het vlak van AVG-compliance draagt bij aan een gezond privacybeleid dat uiteindelijk bijdraagt aan het vertrouwen van mensen in de organisatie.

Volgens de respondenten zal in 2020 verdere aandacht besteed worden aan awareness van medewerkers en leidinggevenden, het toetsen van verwerkers, het toetsen en verbeteren van alle aspecten van AVG-compliance (plan-do-check-act cyclus) en het onderhouden van het verwerkingenregister. Daarbij geeft 48% van de respondenten aan dat externe expertise gewenst is.

3. Aandacht voor privacy

3.1 Aandacht van de directie

Het onderzoek in 2019 toonde aan dat directies van retailorganisaties zich terdege bewust waren van het belang van de AVG. Bijna 95% van de respondenten gaf aan dat de aandacht voor de aspecten uit de AVG voldoende tot ruim voldoende was. Dat is in het onderzoek van dit jaar gedaald naar ruim 75%. 20% van de respondenten geeft aan dat de aandacht vanuit de directie voor de AVG nu verslapt.

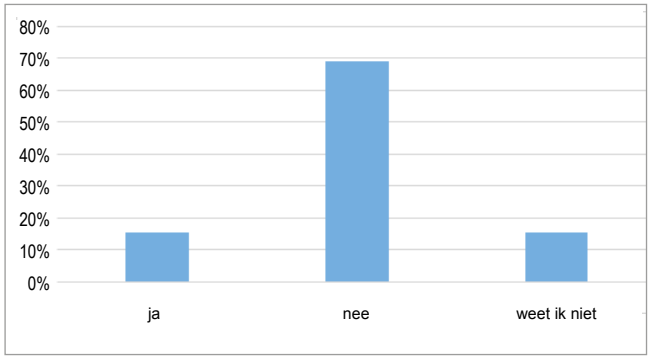
3.2 Aandacht van AP

De rol van de AP verandert. Van vraagbaak, uitleg geven, voorlichting geven, awareness kweken voor de AVG naar waarschuwen, toezichthouden en handhaven. We zien dat terug in de antwoorden. Eén op de zeven respondenten is inmiddels door de AP benaderd. Waarom de AP de organisatie heeft benaderd is niet bekend binnen dit onderzoek. Het tekent wel dat de verschuiving bij de AP naar toezicht en handhaving zichtbaar wordt.

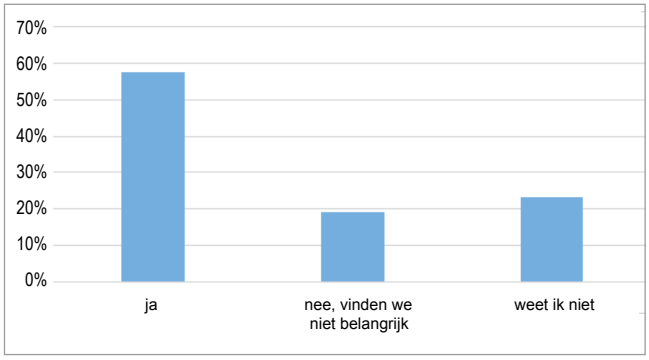
3.3 Aandacht van Consumentenbond

De Consumentenbond toetst middels de Privacy Monitor regelmatig of organisaties zich aan de AVG houden. Zij publiceert de namen van organisaties die zich niet aan de AVG houden en noemt ook de bedrijven die dat wel doen. Voor 57% van de respondenten is dit aanleiding om de naleving van de AVG strakker uit te voeren. 20% van de respondenten vindt het oordeel van de Consumentenbond niet belangrijk en 23% geeft aan niet te weten wat het beleid op dit terrein is.

Benaderd door AP



Benaderd door Consumentenbond



Voorbeelden van handhaven en beboeten:
€725.000,- boete voor een bedrijf voor de onjuiste verwerking van vingerafdrukken personeel.
€525.000,- boete voor de KNLTB voor verkoop ledengegevens.
Duitse toezichthouder:
€35.000.000,- boete voor H&M voor onzorgvuldig verwerken persoonsgegevens van personeel.

4. Informatiebeveiliging

4.1 Informatiebeveiligingsbeleid

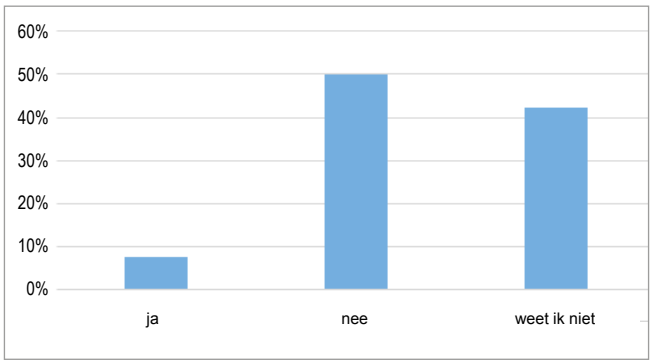
Informatiebeveiliging en privacy zijn nauw met elkaar verbonden. De AVG stelt dat bedrijven effectieve technische en organisatorische beschermingsmaatregelen voor de verwerking van persoonsgegevens moeten treffen. Omdat 15% van de respondenten geen informatiebeveiligingsbeleid heeft en 15% aangeeft niet te weten of er informatiebeveiligingbeleid is, lijkt bij 30% van de respondenten informatiebeveiliging geen tot weinig aandacht te krijgen.

In een tijdperk waarin cyber attacks aan de orde van de dag zijn, is het belangrijk dat een organisatie de beveiliging van haar informatie in het algemeen en persoonsgegevens in het bijzonder, serieus neemt. Bij 70% van de respondenten is dat het geval, maar bij 30% van de respondenten zijn verbeteringen mogelijk. Zeker omdat bij de huidige aanvallen de (financiële) schade flink kan oplopen en in geval van ransomware aanvallen systemen volledig ontoegankelijk kunnen worden. Niet alleen resulteert dat in een datalek, maar zo'n aanval kan ook de continuïteit van organisaties bedreigen. Zonder informatietechnologie kunnen de meeste organisaties niet functioneren.

4.2 Aandacht directie

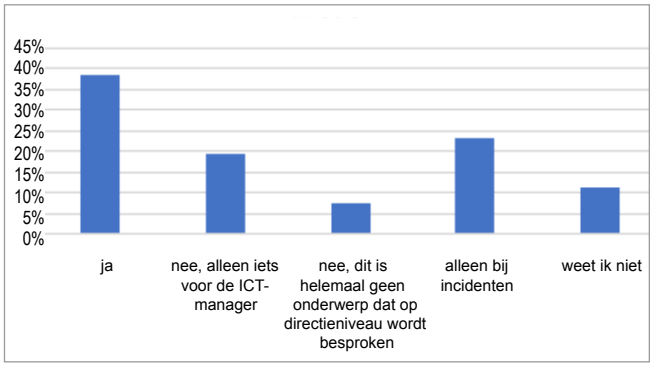
70% van de respondenten geeft aan weliswaar te beschikken over een informatiebeveiligingsbeleid, slechts 8% beschikt daarbij over een ISMS (information security management system.

Beschikt over een ISMS



Een ISMS is een systematische aanpak om informatiebeveiliging continu te beoordelen en waar nodig verbeteringen door te voeren. Dit behoeft duidelijk aandacht binnen de retailsector. Zeker ook omdat 62% van de respondenten aangeeft dat informatiebeveiliging geen onderwerp op de agenda van de directie is. Informatiebeveiliging komt alleen op de agenda bij incidenten of is helemaal geen agendapunt binnen de directie. Een kleine 20% van de respondenten geeft aan dat dit een onderwerp is dat thuishoort binnen de IT-afdeling. Naar onze mening is informatiebeveiliging allang geen specialisme dat voorbehouden is aan een select groepje professionals: het hoort bij de taken en verantwoordelijkheden van elke manager en medewerker. Bovendien kunnen we hier ook aangeven dat niet alleen de eigen informatie-beveiliging op orde dient te zijn, maar ook die van de externe dienstverleners aan wie we de verwerking van persoonsgegevens geheel of gedeeltelijk hebben overgedragen, de zogenaamde verwerkers.

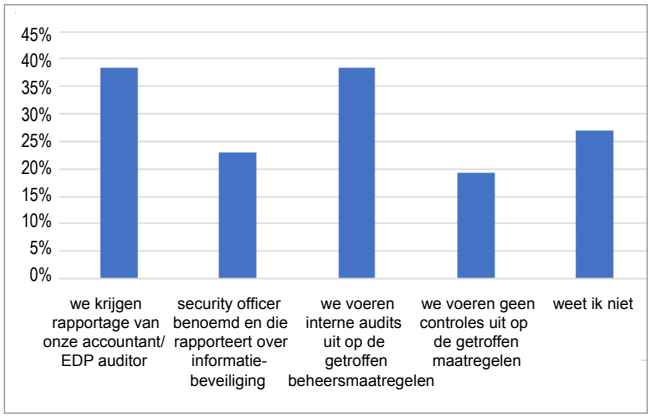
Staat informatiebeveiliging op de agenda van de directie?



4.3 Interne toetsing getroffen maatregelen

Een belangrijke verplichting van verwerkings-verantwoordelijken is het treffen van technische en organisatorische maatregelen om te kunnen waarborgen en aantonen dat de verwerking van persoonsgegevens in overeenstemming is met de AVG. Dat betekent dat beveiligingsmaatregelen periodiek getoetst moeten worden op effectieve werking. 46% van de respondenten geeft aan dat de beveiligingsmaatregelen niet worden gecontroleerd of niet weet dat er controles worden uitgevoerd. De overige 55% van de respondenten toetst op verschillende manieren door bijvoorbeeld onder-zoeken door een accountant/EDP-auditor en/of onderzoeken door de Security Officer en/of door interne audits uit te laten voeren.

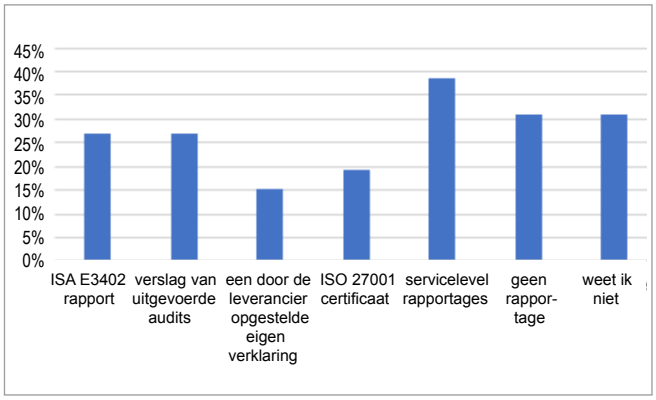
Toetsing beveiligingsmaatregelen intern



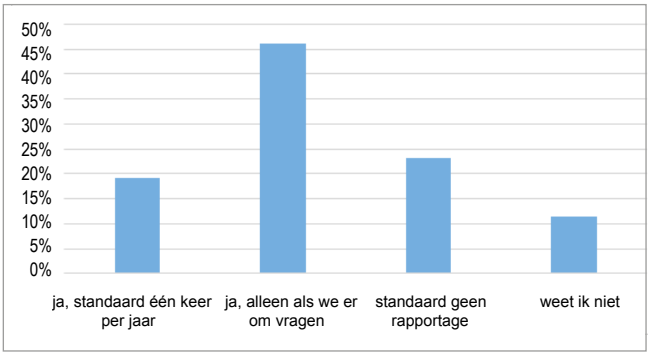
4.4 Toetsing bij diensverleners

Wanneer bedrijven specifieke diensten uitbesteden, is het noodzakelijk dat de dienstverlener zijn opdrachtgever jaarlijks informeert over de stand van informatiebeveiliging. Daarvoor worden verschillende soorten rapportages gebruikt (ISAE3402, door de verwerker opgestelde eigen verklaring, enz.). Opvallend is dat 23% van de respondenten aangeeft geen rapportages te ontvangen. 12% weet niet of de dienstverlener wel rapporteert over de getroffen maatregelen op het gebied van informatiebeveiliging. Dat betekent dat 35% niet over informatie beschikt over de effectiviteit van getroffen maatregelen. Geen bericht is goed bericht maar om verantwoording te kunnen afleggen, is dat niet voldoende.

Soorten rapportage externe dienstverleners



Hoe vaak rapporteren dienstverleners



Conclusie

De conclusie is dat een groot deel van de respondenten niet voldoende in control is over informatiebeveiliging. Dit geldt voor zowel de eigen, interne dienstverlening als voor de externe leveranciers. Daarmee lopen die retail-organisaties een belangrijk risico en wordt niet voldaan aan de AVG.

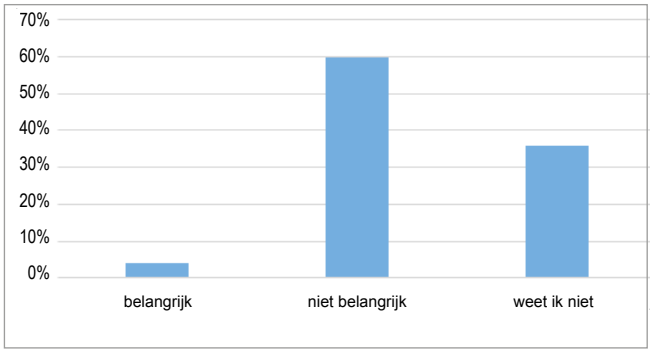
5. Certificering

5.1 Certificering informatiebeveiliging

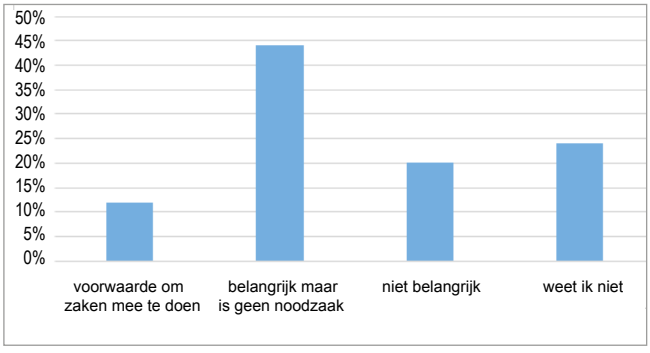
Een organisatie kan aan haar klanten en andere stakeholders aantonen dat zij goed met de informatie-beveiliging omgaat door een ISO 27001 certificering te verkrijgen. 60% van de respondenten vindt een ISO 27001 certificering niet belangrijk. 4% van de respondenten vindt het belangrijk en 36% weet het niet. Kortom, certificering van de maatregelen op het terrein van informatiebeveiliging heeft geen prioriteit en krijgt weinig aandacht. Dat blijkt ook uit het feit dat er geen enkele respondent ISO 27001 gecertificeerd is.

Veel retailorganisaties hebben grote delen van de ICT uitbesteed en de vraag is dan of retailers van de ICT-dienstverleners vereisen dat informatie-beveiliging bij de ICT dienstverlener op orde is. Een dienstverlener kan dat aantonen door een ISO 27001 certificaat. Voor 12% van de respondenten is een ISO 27001 certificaat een voorwaarde om zaken te kunnen doen met een ICT-dienstverlener. Voor 44% van de respondenten is het wel belangrijk maar geen noodzaak om zaken te doen met een ICT-dienstverlener. 20% geeft aan dat certificering van de ICT-dienstverlener niet belangrijk is.

Belang aantonen eigen ISO 27001



Belang ISO 27001 bij ICT-dienstverleners



Is een ISO 27001 certificaat voldoende om privacy-naleving aan te tonen door verwerkers?

Als u processen uitbesteedt aan een dienstverlener (verwerker), mag u alleen in zee gaan met verwerkers die aantoonbaar aan de AVG (blijven) voldoen (art 28 lid 1 AVG). Ter verantwoording van de naleving van de AVG wordt certificering volgens informatiebeveiligingsstandaard ISO 27001 steeds vaker aangehaald door verwerkers. Geeft het ISO 27001 certificaat voldoende zekerheid dat privacy-maatregelen passend zijn en structureel worden toegepast?

Het antwoord is nee. De doelstellingen van informatiebeveiliging richten zich primair op de kwaliteits-aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Privacyspecifieke vraagstukken gebaseerd op de rechten van betrokkenen en verantwoordelijkheid van organisaties ontbreken. Zo bevat informatiebeveiliging geen beheerdoelstellingen gericht op inzage, dataportabiliteit, verwerkers-overeenkomsten, register van verwerkingen, anonimisering, bewaartermijnen en datalekken. Het zijn juist deze verplichtingen die het onderscheid maken tussen informatiebeveiliging en privacy. Informatiebeveiliging is een belangrijk thema binnen de AVG, maar privacy vraagt meer dan informatiebeveiliging alleen.

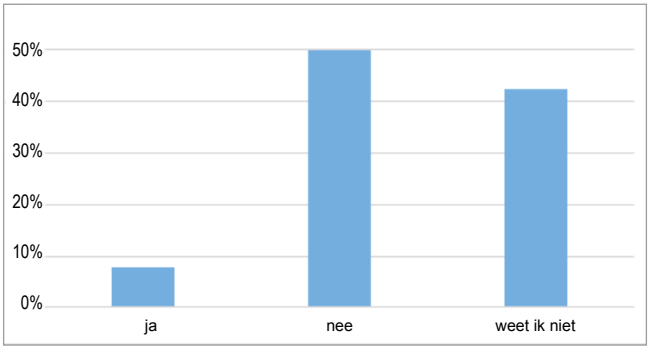
Een ISO 27001 certificering beoordeelt of een organisatie een adequaat Information Security Management System (ISMS) heeft geïmplementeerd. Dat betekent dat het ontwerp van de maatregelen (opzet) en uitvoering (bestaan) kan worden aangetoond op het moment van certificering.
De certificering beoordeelt niet of de beveiliging van informatie gedurende een langere periode (bijvoorbeeld een kalenderjaar) goed heeft gewerkt (werking).

Wil een verwerker de opdrachtgever zekerheid (assurance) verstrekken over informatiebeveiliging en privacy, dan kan deze kiezen voor ISAE 3400 audit. De International Standard for Assurance Engagements (ISAE) is een internationale assurance verklaring die in Nederland door register-accountants (RA) en register IT-auditors (RE) wordt toegepast. In de ISAE 3402 rapportage wordt een uitspraak gedaan over het ontwerp en de structurele uitvoering gedurende een bepaalde periode (werking) van die maatregelen. In tegenstelling tot het ISO 27001 certificaat, geeft deze rapportage de opdrachtgever zekerheid (assurance) dat de verwerking van persoonsgegevens in overeenstemming met de AVG is uitgevoerd, zoals gesteld in artikel 24 van de AVG, mits het beoordelen van privacy aspecten in de scope van de ISAE 3400 opdracht is opgenomen.

5.2 AVG certificering

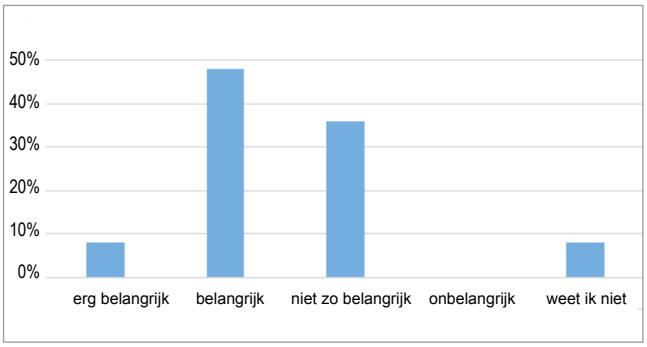
Met een AVG-certificaat toont een organisatie aan de AVG na te leven en de privacy van haar klanten te respecteren. Diverse certificeringsorganisaties zijn actief om een AVG certificaat goedgekeurd te krijgen door de AP. Wanneer een AVG certificering voorhanden is, dan is de vraag of retailorganisaties daarvan gebruikt gaan maken.

Maken retailorganisaties gebruik van AVG-certificering?



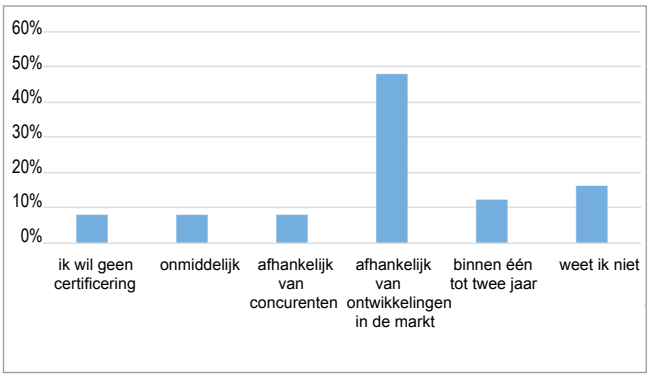
Belangrijk in de afweging om wel of niet een AVG-certificaat te behalen, is de vraag hoe belangrijk de klanten van retailorganisaties een dergelijke certificering vinden. 56% van de respondenten denkt dat de klanten een dergelijke certificering (zeer) belangrijk vinden. 36% denkt dat klanten hier niet zo veel waarde aan hechten.

AVG-certificering belangrijk voor klanten?



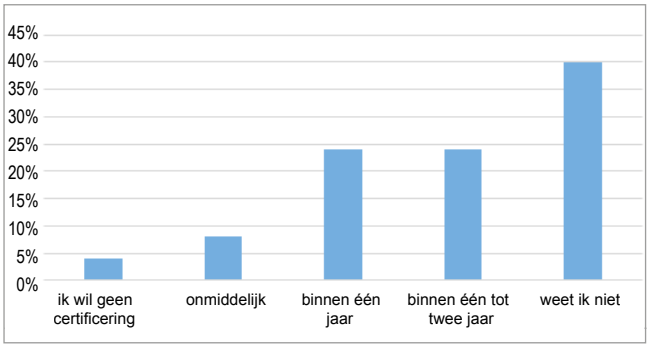
Wanneer het mogelijk is een AVG-certificaat te behalen is slechts een klein deel (8%) van de respondenten van plan daar direct actie op te ondernemen. Ongeveer de helft van de respondenten kijkt eerst de kat uit de boom en wacht de ontwikkelingen in de markt af.
Als echter de brancheverenging certificering ondersteunt, zien we een ander beeld waarbij meer retailorganisaties aangeven een AVG-certificaat te willen behalen. 56% wil dan binnen 2 jaar kunnen beschikken over een AVG-certificaat. 40% van de respondenten heeft nog niet stil gestaan bij deze vraag. Een heel klein aantal respondenten geeft aan geen AVG-certificaat te willen behalen.

Wanneer AVG-certificering?



Wanneer AVG-certificering in Nederland tot de mogelijkheden behoort, is dat ook belangrijk voor de verwerkers. Voor 12% van de respondenten is een dergelijk certificaat een voorwaarde om zaken te doen met een verwerker. 72% vindt het belangrijk dat een verwerker beschikt over een AVG-certificaat maar het is nu nog geen noodzakelijke voorwaarde.

Wanneer AVG-certificering als verplicht ?



Welke typen dienstverleners dienen AVG-gecertificeerd te zijn volgens onze respondenten? ICT-dienstverleners voeren de ranglijst aan, gevolgd door HR-dienstverleners en marketingbureaus.
De accountant scoort aanzienlijk lager. Dat is niet verwonderlijk, want de accountant kent al strenge beroepsvoorwaarden (NBA) en hoeft niet door middel van een apart certificaat aan te tonen dat de zaken op orde zijn.

6. Over Contakt Consulting

Contakt Consulting adviseert bedrijven over informatietechnologie en helpt haar klanten daar optimaal gebruik van te maken. Elk vraagstuk vergt zijn eigen aanpak en expertise. Contakt Consulting bestaat daarom uit een uitgebreid netwerk van professionals met specifieke kennis en jarenlange ervaring. Zij hebben hun strepen verdiend in sectoren als retail, foodbedrijven, bouwnijverheid, logistiek en industrie. Door expertises te bundelen lossen we multidisciplinaire vraagstukken effectief op.

6.1 Retail diensten van Contakt Consulting

Contakt Consulting heeft meer dan 20 jaar ervaring met retailers en het vertalen van business vraagstukken naar IT-oplossingen. Onze retailexperts ondersteunen u graag bij het beantwoorden van vragen over de verbeteringen, veranderingen en samenwerkingen in retail zowel strategisch, tactisch als operationeel. Zij zijn onafhankelijk en kennen de markt met IT-oplossingen. Desgewenst vullen wij ad interim rollen in om uw organisatie een boost te geven, of nemen we de verantwoordelijkheid om een programma of project succesvol op te leveren.

6.2 Privacy diensten voor de retail

Om retailers te kunnen ondersteunen bij het evalueren van hun AVG-compliance, heeft Contakt Consulting onder meer een Privacy Scan ontwikkeld. Daarnaast bieden we methodes om medewerkers te laten oefenen met datacalamiteiten. De resultaten uit de scan, de oefeningen en de praktijk geven aan op welke punten u uw AVG compliance verder kan versterken. Contakt Consulting kan u incidenteel ondersteunen op specifieke onderwerpen als awareness, het uitvoeren van DPIA's, het uitvoeren van een phishing test en het controleren van verwerkers. Voor structurele ondersteuning kunt u gebruik maken van de privacy officer in abonnements-vorm. Daarmee bent u met de inzet van een beperkt aantal dagen per maand verzekerd van een ervaren privacy officer met retailkennis. Naast het beantwoorden van alle privacyvragen houden we u ook op de hoogte van relevante ontwikkelingen op het gebied van privacy.

6.3 Retail Ronde Tafel

Contakt Consulting organiseert periodiek Retail Ronde Tafels rondom verschillende thema's, zoals "De achter-kant van omnichannel", "Master Data Management", "Is er toekomst voor de kassa" en "AVG". Onder begeleiding van specialisten worden ervaringen, vraagstukken en best practices besproken. Retailers die de Tafel al eerder hebben bijgewoond zijn unaniem enthousiast over deze kennissessies. De bijeenkomsten staan open voor alle betrokken professionals in de retailsector.

6.4 Vragen?

Bent u benieuwd hoe onze retail experts uw organisatie kunnen ondersteunen?
Neem dan contact op met Ronald van Putten, +31 6 29 09 1602 of ronald.van.putten@contakt.nl.

7. Het privacyteam

Deze benchmark is tot stand gekomen door de volgende personen die uitmaken van het privacy team van Contakt Consulting:

Dick Sepers
Sales

Ronald van Putten
Directeur Contakt Consulting

Lodewijk Benjaminse
Privacy en security consultant

Ad Boumans
Privacy en security consultant

Douwe Douma
Privacy en security consultant

René van Eijk
Privacy en security consultant

Contakt Consulting BV

Atoomweg 50, 3542 AB Utrecht
Telefoon: +31 (0)88 303 11 00
E-mail: info@contakt.nl
Website: www.contakt.nl