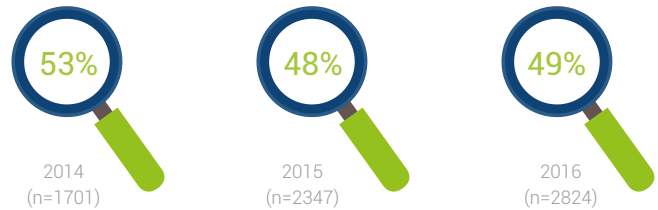
DE ACHT DINGEN DIE U MOET WETEN OVER DE GENERAL DATA PROTECTION REGULATION (GDPR)

SECURE MY DATA

Iedereen heeft recht op bescherming van zijn of haar persoonsgegevens. De EU-lidstaten hebben nu nog hun eigen nationale wetten, gebaseerd op de Europese privacyrichtlijn uit 1995. Per 25 mei 2018 wordt deze echter vervangen door een nieuwe wet: General Data Protection Regulation (GDPR, ook wel de algemene verordening gegevensbescherming (AVG) genoemd). Er is dan nog maar één privacywet in de hele EU. Veel bedrijven voldoen nog niet aan de gestelde eisen, terwijl de sancties ingrijpend kunnen zijn. Wees goed voorbereid!

Als reactie op de toenemende dreiging van cybercriminaliteit en het groeiende aantal datalekken, spenderen overheden en bedrijven steeds meer budget aan IT-beveiliging. Om initiatieven en innovaties op het gebied van cybersecurity te stimuleren steekt de Europese Commissie 450 miljoen euro in privaat-publieke samenwerking. Branches moeten daarmee de beschikking krijgen over een betere beveiliging tegen cybercriminaliteit. Daartoe heeft Europees Commissaris Günther Oettinger een overeenkomst getekend met de European Cyber Security Organisation. De verwachting is dat de totale investeringen van dit samenwerkingsverband in 2020 uitkomen op minimaal 1,8 miljard euro. De Europese Commissie vindt publiek-private samenwerking van belang, omdat 80 procent van alle bedrijven wel eens problemen met cybercriminaliteit heeft ondervonden en alleen een gezamenlijke aanpak effectief is. Het aantal cyberincidenten is vorig jaar met 38 procent gestegen en geen sector is uitgesloten van digitale dreiging. Het richten van de focus op security lijkt nu belangrijker dan ooit tevoren.

Het percentage organisaties dat publiekelijk met een datalek te maken heeft gehad.



BRON:

Cisco 2017 Security Capabilities Benchmark Study

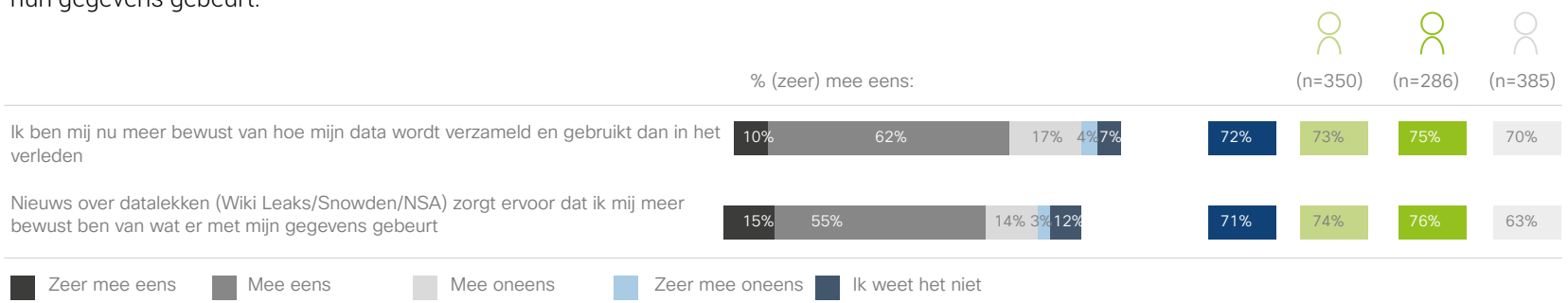
De grootste zorgen van security-medewerkers met betrekking tot cyberaanvallen

BRON:

Cisco 2017 Security Capabilities Benchmark Study

PRIVACY EN GEGEVENSVERZAMELING HOT TOPIC

De snelle technologische ontwikkelingen en het stijgende aantal mobiele devices hebben de verhouding tussen de consument en organisaties getransformeerd. Mensen hebben op internet toegang tot een oneindige schat aan informatie die hen helpt beslissingen te nemen. De mogelijkheid om informatie te delen draagt bij aan deze consumentenemancipatie. Er is daardoor steeds meer bewustwording over gegevensverzameling. Zeven van de tien consumenten geven aan zich er, meer dan in het verleden, van bewust te zijn dat hun data wordt verzameld. Nieuws over datalekken, onder meer verspreid door Edward Snowden en WikiLeaks heeft ervoor gezorgd dat mensen zich meer bewust zijn van wat er met hun gegevens gebeurt.



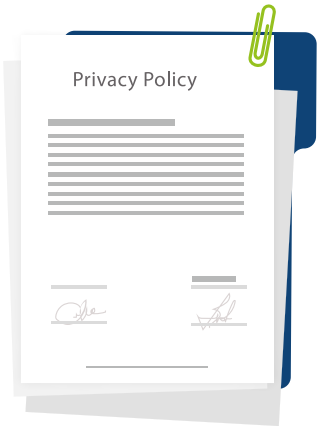
BRON:

DDMA: privacy onderzoek 2016

GENERAL DATA PROTECTION REGULATION (GDPR)

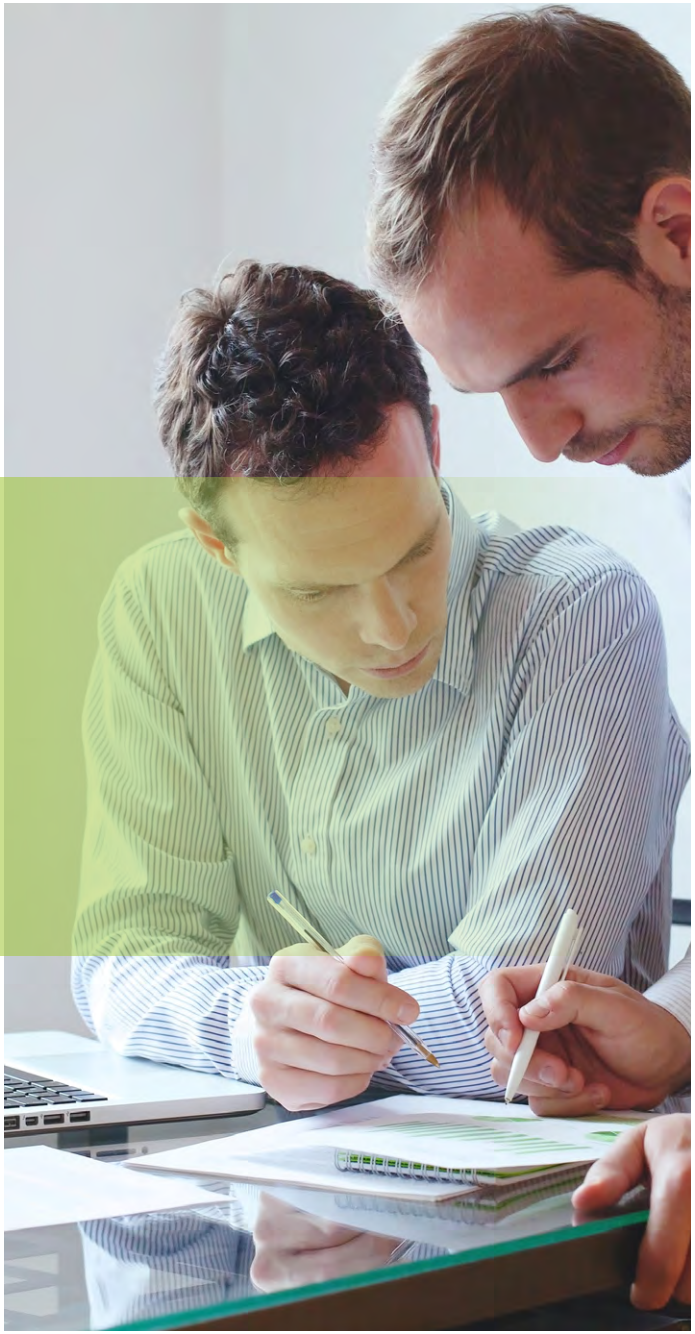
De GDPR vervangt de databeschermingsrichtlijn uit 1995. De reden is dat de verouderde richtlijn uit 1995 niet meer aansluit op de huidige digitale wereld. De GDPR is in mei 2016 in werking getreden en organisaties hebben tot en met 25 mei 2018 de tijd om hun bedrijfsvoering met de GDPR in overeenstemming te brengen. Opsporingsinstanties en het OM zijn vrijgesteld van de nieuwe verordening omdat zij onder aparte privacywetgeving vallen. De GDPR zorgt onder meer voor:

- versterking en uitbreiding van privacyrechten;
- meer verantwoordelijkheden voor organisaties;
- dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders.



ACHT DINGEN DIE U MOET WETEN OVER DE GDPR

Het is zaak om goed voorbereid te zijn op de nieuwe verordening. Niets doen is geen optie, want de boetes die geriskeerd worden zijn enorm. Om u te ondersteunen bij de voorbereidingen stippen we acht zaken over de GDPR aan die belangrijk zijn om te weten.



1. BELANGRIJKE DATA

Om u wat meer inzicht te geven, schetsen we allereerst een beeld van wat wanneer heeft plaatsgevonden omtrent de GDPR. Op 4 mei 2016 is de verordening gepubliceerd in het Publicatieblad van de Europese Unie. Twintig dagen na deze publicatie is het in werking getreden, maar pas vanaf 25 mei 2018 is het van toepassing. Er zit dus een periode van twee jaar tussen de inwerkingtreding van de GDPR en het moment dat deze daadwerkelijk van toepassing is. Deze tijd is nodig om organisaties en toezichthouders zich goed te laten voorbereiden op de GDPR. Gedurende deze twee jaar geldt in Nederland nog steeds de Wet bescherming persoonsgegevens.

21 oktober 2013	*Introductie in het Europees Parlement*
2013 - 2015	*Onderhandelingen tussen het Europees Parlement, de Raad en de Commissie*
24 mei 2016	*GDPR is in werking getreden*
24 mei 2016 - 24 mei 2018	*Implementatieperiode*
6 mei 2018	*EU-lidstaten moeten de verordening hebben omgezet in nationale wetgeving*
25 mei 2018	*Organisaties zijn aanspreekbaar op naleving*

2. DE PRINCIPES

De uitgangspunten van de GDPR zijn gebaseerd op vier principes:

1. Wettelijke grondslag
Verwerkingen van persoonsgegevens mogen alleen plaatsvinden wanneer daarvoor a) ondubbelzinnige toestemming door betrokkene is verleend, of b) dit noodzakelijk is voor een aantal limitatief opgesomde belangen.

2. Doelbinding
Persoonsgegevens mogen alleen verwerkt worden voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden en niet zomaar voor andere doeleinden.

3. Dataminimalisatie
Er mogen niet meer persoonsgegevens verwerkt worden dan noodzakelijk.

4. Passende beveiliging
Verwerkers van persoonsgegevens dienen passende technische en organisatorische maatregelen te nemen om de verwerking te beveiligen.

3. BELANGRIJKSTE VERSCHILLEN VOOR ORGANISATIES

Bij de GDPR wordt meer nadruk gelegd op de verantwoordelijkheid van organisaties zelf, om de wet na te leven én om te kunnen aantonen dat ze zich aan de wet houden. Ze moeten daarom voldoen aan een documentatieplicht. Dit houdt in dat organisaties met documenten moeten kunnen aantonen dat ze de juiste maatregelen hebben genomen om aan de wet te voldoen. De GDPR biedt organisaties meer instrumenten om ze te helpen de wet na te leven. Bijvoorbeeld modelbepalingen voor de relatie tussen de verantwoordelijke en de verwerker en voor doorgifte van persoonsgegevens. Zodra de GDPR op 25 mei 2018 van kracht gaat, verandert het volgende:

- organisaties kunnen verplicht worden een privacy impact assessment (PIA) uit te voeren;
- organisaties kunnen verplicht worden een functionaris voor de gegevensbescherming (FG) aan te stellen;
- verwerkingen van persoonsgegevens hoeven niet meer bij de Autoriteit Persoonsgegevens gemeld te worden.

4. DE PIA EN WANNEER U DIE MOET UITVOEREN

U voert een PIA uit om in kaart te brengen welke privacyrisico's bijvoorbeeld een bepaald plan, proces of toepassing met zich meebrengt. Als u persoonsgegevens verwerkt en dit een groot risico voor de privacy oplevert voor de mensen van wie u persoonsgegevens verwerkt, is een PIA verplicht. Een PIA is met name vereist:

- wanneer sprake is van een systematische en uitvoerige beoordeling van persoonlijke aspecten van personen, waaronder profilering;
- indien op grote schaal bijzondere persoonsgegevens worden verwerkt, zoals medische of strafrechtelijke gegevens;
- als op grote schaal en systematisch mensen worden gemonitord in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

De Autoriteit Persoonsgegevens gaat samen met de andere Europese privacytoezichthouders nog een lijst opstellen van alle soorten verwerkingen waarbij u verplicht bent om een PIA uit te voeren.

5. FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING (FG)

De verplichting om een FG aan te stellen geldt alleen voor publieke instanties en organisaties waarbij de aard van de verwerking daar aanleiding toe geeft, of in geval van grootschalige verwerking van bijzondere gegevens. Andere organisaties hebben de vrijheid om zelf te kiezen of ze wel of geen functionaris aanstellen. Gaat u een FG aanstellen? Let dan op de volgende zaken:

- aanstelling o.b.v. professionele kwaliteiten en inhoudelijke expertise van het recht en de praktijk;
- rapporteert rechtstreeks aan het management;
- wanneer ook andere taken vervuld worden door de FG, dan mag dit niet tot een belangenconflict leiden;
- de FG kan een fulltime of parttime functie zijn en zowel intern of extern;
- de FG mag ook door een groep van ondernemingen worden aangewezen.

Het advies luidt om vroeg met het vormgeven van de rol van de FG binnen uw organisatie te beginnen, zodat deze op tijd ingevuld is.

6. WAT MERKEN MENSEN VAN WIE PERSOONSGEGEVENS WORDEN VERWERKT VAN DE GDPR?

Dankzij de GDPR krijgen mensen meer mogelijkheden om bij de verwerking van hun gegevens voor zichzelf op te komen. In de GDPR staat bijvoorbeeld een artikel over toestemming waarin de voorwaarden voor organisaties om geldige toestemming te kunnen krijgen om persoonsgegevens te verwerken staan vermeld. Zo moeten organisaties bewijzen dat ze toestemming hebben en moeten mensen de mogelijkheid hebben om hun toestemming ook weer in te trekken. Ook krijgen mensen door de GDPR een aantal aanvullende rechten. Behalve het recht om hun persoonsgegevens te laten verwijderen, kunnen ze eisen dat de organisatie de verwijdering doorgeeft aan alle andere organisaties die deze gegevens van de desbetreffende organisatie hebben gekregen. Daarnaast hebben mensen straks het recht om hun persoonsgegevens in een standaardformaat te ontvangen. Zo kunnen zij hun gegevens makkelijk doorgeven aan een andere leverancier van dezelfde soort dienst. Bijvoorbeeld als zij zich willen uitschrijven bij de ene sociale netwerksite en zich inschrijven bij een andere. Zij kunnen zelfs eisen dat de organisatie hun persoonsgegevens direct doorstuurt aan de nieuwe dienstverlener.

7. WAT LEVERT DE GDPR U ALS ORGANISATIE OP?

Als de GDPR van toepassing is, geldt er nog maar één privacywet in de hele Europese Unie in plaats van 28 verschillende nationale wetten. Als u persoonsgegevens verwerkt hoeft u zich nog maar aan één Europese wet te houden. Bent u in meerdere EU-lidstaten actief? Dan levert de GDPR u het volgende op:

- u heeft minder administratieve kosten en nalevingskosten;
- u heeft meer rechtszekerheid;
- er is een gelijk speelveld (level playing field), want alle regels zijn hetzelfde voor alle bedrijven in de EU;
- u hoeft nog maar met één toezichthouder zaken te doen (onestopshop).

8. MOGELIJKE SANCTIES

Zoals eerder aangegeven is het belangrijk om goed voorbereid te zijn op de nieuwe wet GDPR, omdat de gevolgen anders ingrijpend kunnen zijn. Wat zijn de sanctiemogelijkheden en administratieve boetes die de toezichthoudende autoriteiten kunnen opleggen aan bedrijven die niet goed voorbereid zijn? De autoriteiten kunnen:

- de verantwoordelijke of bewerker berispen, indien een verwerking inbreuk maakt op de verordening;
- de verantwoordelijke of bewerker bevelen de verzoeken van betrokkenen tot uitoefening van diens rechten op grond van de verordening in te willigen;
- de verantwoordelijke of bewerker bevelen binnen een bepaalde termijn verwerkingen in overeenstemming te brengen met de verordening;
- de verantwoordelijke bevelen een inbreuk aan de betrokkene te melden;
- een tijdelijke of definitieve verwerkingsverbod opleggen;
- een rectificatie of het wissen van gegevens bevelen;
- de certificering intrekken;
- een administratieve geldboete opleggen;
- gegevensstromen naar derde landen of internationale organisaties opschorten;

Daarnaast hebben ze de bevoegdheid om flinke administratieve boetes op te leggen. Deze kunnen oplopen tot €20 miljoen of 4 procent van de totale wereldwijde jaaromzet in het voorgaande boekjaar indien dit cijfer hoger is. Deze boetes kunnen worden opgelegd naast of in plaats van de hierboven genoemde maatregelen.

BRON:

Cisco 2017 Annual Cybersecurity Report

https://www.ncsc.nl/actueel/nieuwsberichten

http://www.consilium.europa.eu/nl/policies/data-protection-reform/data-protection-regulation/

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving

NOREA, Handreiking PIA: https://www.norea.nl/download/?id=522

https://www.privacycompany.eu/samenvatting-eerdere-blogposts-over-de-privacyverordening/

DDMA: privacy onderzoek 2016

https://zenn.law/algemene-verordening-gegevensbescherming-GDPR-verplichte-overdraagbaarheid-van-gegevens