www.pwc.com

GDPR en reclamerecht

28 november 2017

28 november 2017

pwc

1. PwC visie op GDPR

De GDPR leidt tot een uniforme bescherming van gegevens binnen de gehele Europese Unie

De GDPR is een nieuwe EU Verordening die verder gaat dan de wetgeving inzake bescherming van persoonsgegevens zoals opgenomen in de huidige Wet bescherming persoonsgegevens (Wbp) die is gebaseerd op de Richtlijn 95/46/EC. De GDPR streeft naar gelijke en verbeterde bescherming van persoonsgegevens binnen de gehele Europese Unie. De verordening omvat belangrijke en nieuwe vereisten voor het omgaan met persoonsgegevens zoals het verzamelen, bewerken, gebruiken, bewaren en verspreiden van gegevens.

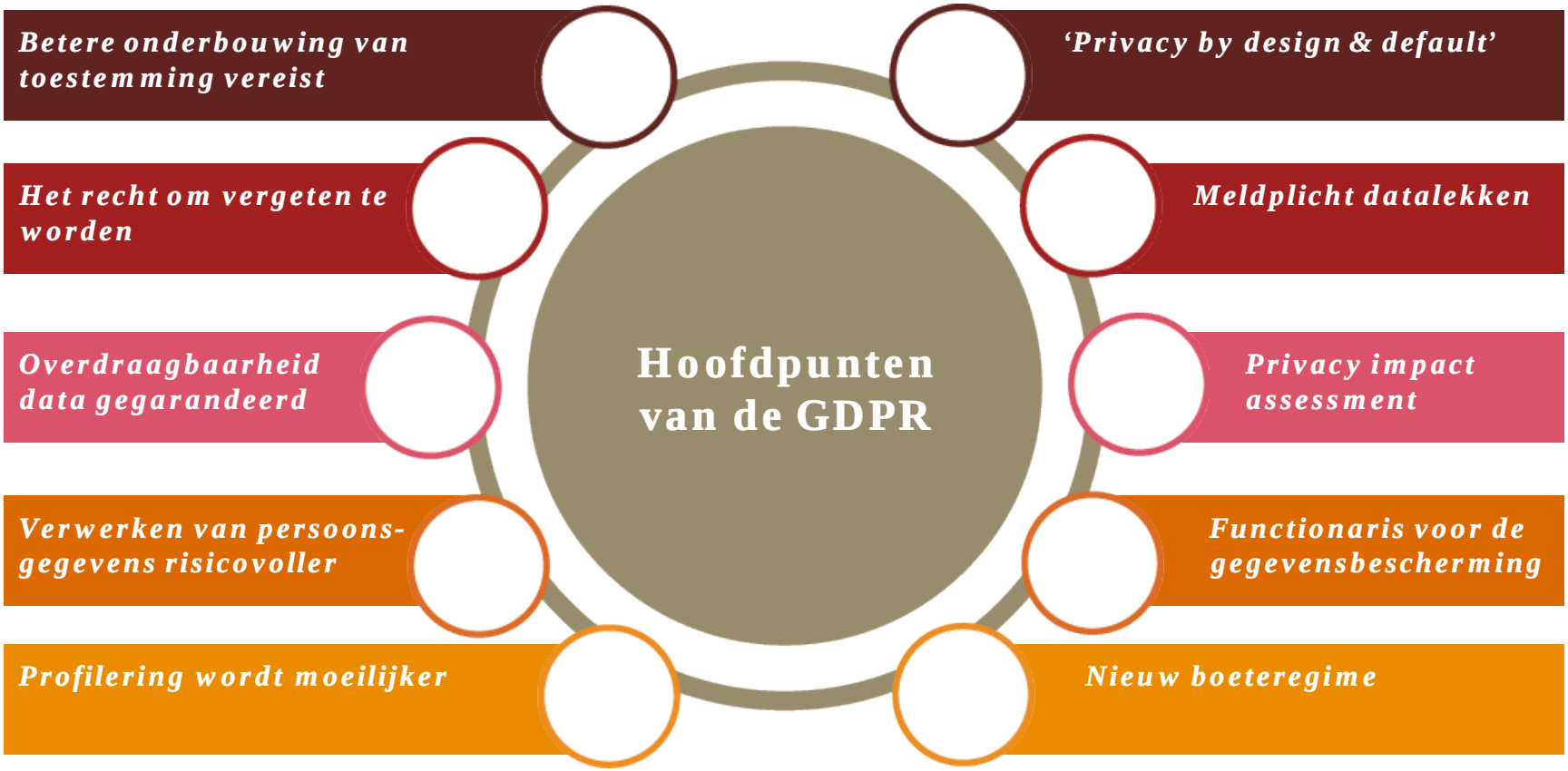
Daarnaast zijn de boetes aanzienlijk verhoogd voor organisaties die niet voldoen aan de vereisten van de GDPR (tot het meerdere van 20 mio euro of 4% van de totale (wereldwijde) jaaromzet).

De GDPR is van toepassing op alle organisaties die persoonsgegevens onder zich houden en deze verwerken binnen de Europese Unie.

Daarnaast heeft de GDPR een extraterritoriaal effect.

Wat verandert er? De GDPR in een notendop

Vanaf 25 mei 2018 zal de General Data Protection Regulation (GDPR) van kracht worden, maar wat verandert er precies? De tien punten uit de GDPR met de grootste impact op organisaties zijn in de visie van PwC de volgende:



Impact op het reclamerecht

Van de 10 belangrijkste thema's uit de GDPR springen er voor het reclamerecht een aantal uit. Deze thema's hebben we hieronder nader toegelicht.

Grondslagen voor verwerking (art. 6 GDPR)

Er moet een legitieme verwerkingsgrondslag zijn voor het verwerken van persoonsgegevens, bijzondere persoonsgegevens en het doorvoeren van persoonsgegevens naar landen buiten de EU. De verwerking is onder andere rechtmatig indien en voor zover de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden. De betrokkene kan zijn toestemming intrekken (opt-out). Opt-out is niet mogelijk indien de verwerking noodzakelijk is voor de uitvoering van een overeenkomst, om te voldoen aan een wettelijke verplichting en om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen.

Betere onderbouwing van toestemming vereist (art. 7 GDPR)

De individuele consument moet expliciet toestaan dat zijn persoonlijke data mag worden verwerkt. Het van tevoren aanvinken van vakjes en/of aannemen dat toestemming is verleend is niet voldoende. Bedrijven dienen specifiek aan te geven wat met de data gaat gebeuren. Het opsporen van toestemming is verplicht. De gegevensbeheerder moet weten wanneer de toestemming is verleend. Op onjuiste wijze verkregen toestemming leidt tot ongeldigheid van de verwerking van de verkregen persoonsgegevens, hetgeen door de Autoriteit Persoonsgegevens (AP) kan worden gesanctioneerd.

Verwerken van persoons-gegevens risicovoller (art. 21 GDPR)

Betrokkenen krijgen het recht om bezwaar te maken tegen het feit dat hun persoonsgegevens gebruikt worden voor de activiteiten van de desbetreffende organisatie, zoals direct marketing activiteiten. Consumenten krijgen het recht om de over hen verzamelde informatie op te vragen en in te zien. In geval van maatschappelijke onrust rondom bepaalde gegevensverwerkingen, kan dit tot aanzienlijke reputatieschade leiden. De AP kan bovendien opleggen dat verwerkingsprocessen - al dan niet tijdelijk - worden stilgelegd.

Wat is het risico van non-compliance?

Toezichthouders risico

- Boetes en sancties
- Algemene norm van zorgvuldigheid
- Persoonlijke aansprakelijkheid bestuurders
- Controles en onderzoeken Autoriteit Persoonsgegevens

Reputatie risico

- Imago schade
- Verlies van vertrouwen door klanten
- Afname van het aantal klanten
- Verlies van vertrouwen werknemers

Financieel risico

- Verlies van inkomsten
- Kosten van rechtszaken
- Individuele recht om schadevergoeding te vorderen
- Kosten van opschonen gegevens
- Collectieve aanklachten

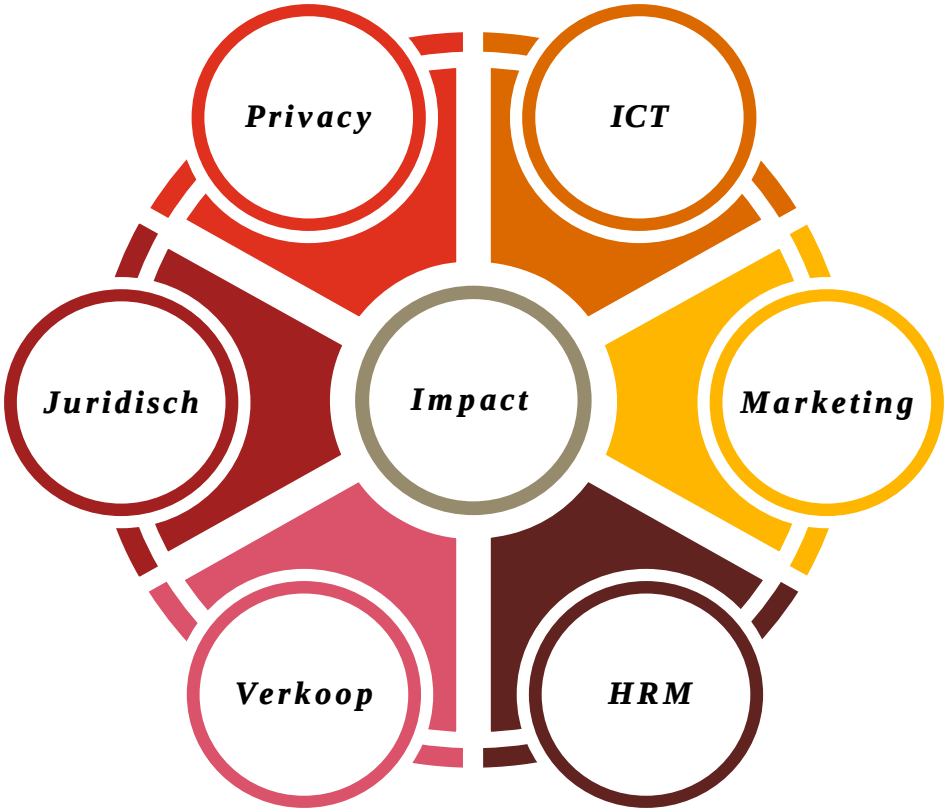
Operationeel risico

- Ongeldige bewerking van gegevens
- Beperkte uitvoering binnen de EU

De impact van de GDPR heeft invloed op de gehele organisatie en is niet beperkt tot een enkele afdeling.

Privacy vereist een benadering vanuit verschillende disciplines en afdelingen.

Bij diverse organisaties zien we dat een effectieve aanpak bestaat uit de oprichting van een stuurgroep - Vaak onder leiding van een bestuurslid - en een projectteam met vertegenwoordigers vanuit alle relevante afdelingen.



PwC Privacy Governance onderzoek

De helft van de organisaties verwacht niet op tijd klaar te zijn voor de Algemene Verordening Gegevensbescherming

Maar **12%** van alle organisaties in Nederland zegt nu al klaar te zijn voor de nieuwe EU-Verordening. Slechts de helft (52%) verwacht vóór de deadline van 25 mei 2018 alle voorbereidingen te hebben afgerond.

12% Klaar!

52% Verwacht de deadline te halen

De opkomst van de privacy officer stagneert

17% van de deelnemers heeft de verantwoordelijkheid voor privacy belegd bij de privacy officer en nog maar **21%** van de organisaties heeft het nergens belegd, of heeft geen privacybeleid.

Mankracht en kennis zijn grootste struikelblok

Als grootste struikelblok voor tijdige implementatie van de noodzakelijke privacy verplichtingen is gebrek aan mankracht **(39%)**, gevolgd door onvoldoende kennis over het onderwerp **(34%)**.

Budgetten voor privacy compliance groeien

50% van de deelnemers geeft aan het afgelopen jaar extra geïnvesteerd te hebben in privacy compliance. De belangrijkste reden hiervoor is dat organisaties zich verantwoordelijk voelen voor de bescherming van persoonsgegevens **(66%)**.

Verwerkingen van persoonsgegevens inzichtelijk, maar niet gedocumenteerd

Bijna **80%** van de organisaties zegt inzichtelijk te hebben welke persoonsgegevens worden verwerkt; maar slechts **45%** documenteert de verwerkingen. Slechts een zeer kleine minderheid van **19%** geeft aan te voldoen aan de verplichting dat alle verwerkingen inzichtelijk en gedocumenteerd zijn.

PwC Privacy Governance onderzoek

Privacy by design lijkt goed ingebed in organisaties

Privacy by Design is inmiddels goed ingebed binnen organisaties. **69%** van de organisaties houdt rekening met gebruik van persoonsgegevens bij introductie van nieuwe systemen.

Bewerkersovereenkomsten worden wel gebruikt, maar veelal niet gecontroleerd

57% van de organisaties geeft aan gebruik te maken van bewerkersovereenkomsten bij inzet van leveranciers.

43% van de organisaties die het niet gebruikt weet niet wat een bewerkersovereenkomst is.

Begrip van de risico's en impact

50% van de deelnemende organisaties voert geen risico analyses (bijvoorbeeld Privacy Impact Assessments) uit in het kader van omgang met persoonsgegevens.

Rechten van betrokkene nog niet goed ingebed

38% heeft geen enkele procedure geïmplementeerd voor de afhandeling van inzage- en correctieverzoeken van betrokkenen.
31% van de organisaties heeft geen bewaartermijnen vastgesteld.

Meldplicht datalekken nog niet goed geïmplementeerd bij organisaties

Een kleine meerderheid **(58%)** voldoet aan de wettelijke verplichting om een centraal overzicht van datalekken bij te houden.

Bijna de helft **(49%)** van de organisaties heeft een draaiboek gereed voor gevallen dat er zich een datalek voordoet.

23% heeft in het afgelopen jaar één of meerdere datalekken gemeld bij de Autoriteit Persoonsgegevens.

De uitdaging lijkt nu vooral om te zorgen dat hetgeen op papier staat wordt omgezet naar de praktijk.

Hartelijk dank.

Yvette van Gemerden
Partner Data Privacy Legal
Phone: +31 (0)88 792 54 42
Mobile: +31 (0)6 **52 00 59 24**
yvette.van.gemerden@pwc.com