NETWORKING4ALL™
the trust provider

Introductie

Met de ingang van de General Data Protection Regulation (GDPR) op 6 mei 2018 wordt de privacy van (persoons)gegevens Europabreed geregeld. Daarmee komt de Nederlandse Wet Bescherming Persoonsgegevens (WBP) te vervallen.

In deze whitepaper wordt er ingegaan op de aankomende veranderingen, beginnende met de samenvatting van de grootste verschillen in vergelijking met de huidige situatie. Deze worden vervolgens nader toegelicht. Tot slot voorziet dit document in een handig stappenplan om GDPR-compliant te worden.

P +31 (0)20 788 10 30 F +31 (0)20 788 10 40 E sales@networking4all.com W www.networking4all.com
PO Box 15320 1001 MH Amsterdam The Netherlands

De grootste veranderingen in hoofdlijnen

Één Europese wetgeving en toezichthouder
Het Nederlandse Autoriteit Persoonsgegevens (AP) en andere nationale autoriteiten worden aangestuurd door een Europese organisatie genaamd European Data Protection Board (EDPB).

Toepassing buiten de EU
De wet is van toepassing als de persoon of organisatie in Europa woonachtig of gevestigd is. Dus ook het opslaan van Europese gegevens in Amerika of China valt onder deze regelgeving.

Privacy als een standaard
Waar gebruikers hun privacy eigenschappen zelf kunnen instellen, moeten deze standaard op de hoogste norm zijn afgesteld.

Assessments
Het uitvoeren van Privacy Impact Assessments (PIA) wordt verplicht. Privacy-risico's moeten streng worden onderzocht. Deze assessments moeten periodiek worden uitgevoerd.

Data Protection Officer
Organisaties van een bepaalde vorm of omvang dienen een Data Protection Officer (DPO) aan te stellen. De DPO moet onafhankelijk opereren en beschikken over kennis van privacywetgeving, informatiebeveiliging en risicomanagement.

Strengere en duidelijke voorwaarden
Eisen aan privacymeldingen worden aangescherpt: bewaartermijnen van persoonsgegevens, contactgegevens van de organisatie en contactgegevens van de DPO moeten duidelijk vermeld worden.

Toestemmingseisen
Personen moeten specifiek toestemming geven voor het verzamelen van informatie en instemmen met het doel, voordat gegevens verwerkt mogen worden. Voor kinderen jonger dan 13 jaar moet de ouder of voogd deze toestemming geven. Toestemming moet altijd weer ingetrokken kunnen worden.

Recht op wijziging
Personen moeten hun persoonlijke gegevens kunnen downloaden in een voor hen begrijpelijk formaat. Onder speciale omstandigheden mogen personen eisen dat hun gegevens worden verwijderd.

Hogere boetes
Boetes voor overtredingen kunnen oplopen tot € 20.000.000,- (of 4% van de jaaromzet als dit bedrag hoger is).

Meldplicht datalekken
In de GDPR wordt het melden van datalekken verplicht gesteld. Nederland kent een vergelijkbare wet die vanaf 1 januari 2016 al van kracht is.

Toelichting

Uiterlijk 6 mei 2018 dienen de EU lidstaten de GDPR op te nemen in het eigen nationale wetboek. Alle bedrijven die persoonsgegevens beheren of verwerken van EU burgers of binnen de EU gevestigde bedrijven dienen per 25 mei 2018 te voldoen aan de wet.

Vanaf het moment dat de GDPR van kracht is zal het Autoriteit Persoonsgegevens (AP) en andere nationale toezichthouders worden aangestuurd door het European Data Protection Board (EDPB). Maar de verantwoordelijkheid strekt verder dan de buitenste Europese grenzen. De wet is tevens van toepassing als de persoon of organisatie niet in Europa woonachtig of gevestigd is.

De wetgeving zal in eerste instantie van toepassing zijn voor organisaties met meer dan 250 werknemers die meer dan vijfduizend records per jaar verwerken. In een later stadium geldt de GDPR ook voor het midden- en kleinbedrijf, ongeacht hun grootte en het aantal records dat ze verwerken.

Richtlijnen

Bedrijven moeten vanaf dat moment toestemming hebben gevraagd aan de betrokkenen voor het verwerken van gegevens. Indien de mate van privacy kan worden ingesteld, dient deze standaard op de strengste instellingen te staan.
Men moet specifiek toestemming worden gegeven voor het verzamelen van informatie door het bedrijf, en instemmen met het doel. Bovendien moet vastgesteld worden dat de verstrekte gegevens proportioneel zijn tot het gewenste doel. Ook na het geven van het akkoord hebben betrokkenen recht op inzage, correctie en verwijdering van hun gegevens.

Het hele verwerkingsproces moet transparant verlopen. Bij elke verwerking van persoonsgegevens wordt een verantwoordelijke aangewezen die erop toeziet dat de verwerking voldoet aan de bijbehorende voorwaarden. Informatie zoals de bewaartermijnen en contactgegevens van de organisatie en verantwoordelijken dienen zichtbaar te worden gepresenteerd. De verwerkingsverantwoordelijke dient passende organisatorische en technische beveiligingsmaatregelen te treffen. Om te voldoen aan de GDPR moet er met een Privacy Impact Assessment (PIA) periodiek worden geïnventariseerd welke privacyrisico's zich voordoen en hier maatregelingen aan koppelen.

De GDPR stelt organisaties bij een bepaalde vorm of omvang verplicht om een functionaris voor de gegevensbescherming aan te stellen. Deze Data Protection Officer (DPO) zorgt voor een correcte verwerking van de (persoons)gegevens. Een DPO dient te worden aangesteld als een organisatie aan één van de onderstaande voorwaarden voldoet:

- Publieke organisaties
- Organisaties die in grote mate systematisch monitoren
- Organisaties die in grote mate gevoelige persoonlijke informatie verwerken

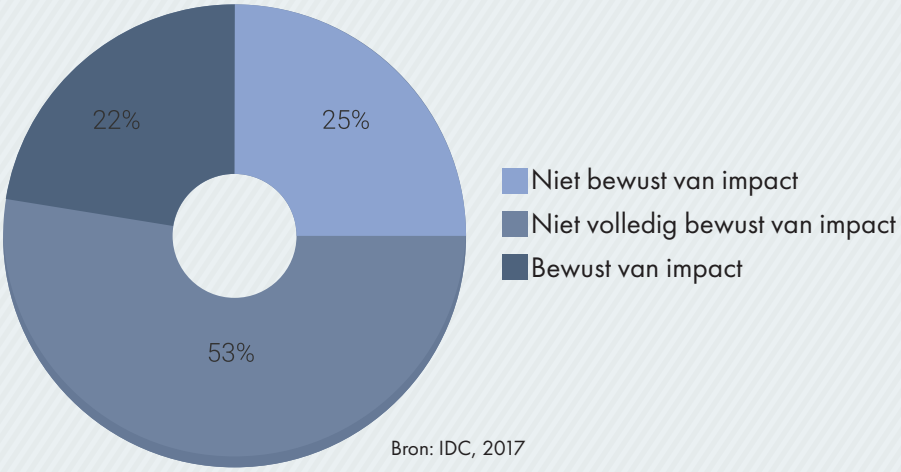
De DPO heeft bevoegdheden om onafhankelijk assessments te verrichten en de naleving van wet- en regelgeving te toetsen. Om deze rol op een bekwame wijze in te vullen dient de DPO te beschikken over kennis van privacywetgeving, informatiebeveiliging en risicomanagement.

Datalek
Bij een datalek is het bedrijf of de organisatie verplicht dit binnen 72 uur te melden aan de toezichthouder en alle betrokkenen. In Nederland is dit sinds 1 januari 2016 geregeld in de wet Meldplicht Datalekken. Wanneer de GDPR van kracht is geldt dezelfde plicht ook voor de overige Europese landen.

Bedrijven die zich niet houden aan de wetgeving zijn strafbaar. De toezichthouder kan een boete opleggen tot € 10.000.000,- of 2% van de totale wereldwijde jaaromzet, indien dit bedrag hoger is. Indien er onvoldoende wordt gehandeld naar de situatie door het bedrijf kan deze boete oplopen tot maar liefst € 20.000.000,- of 4% van de totale wereldwijde jaaromzet, indien dit bedrag hoger is.

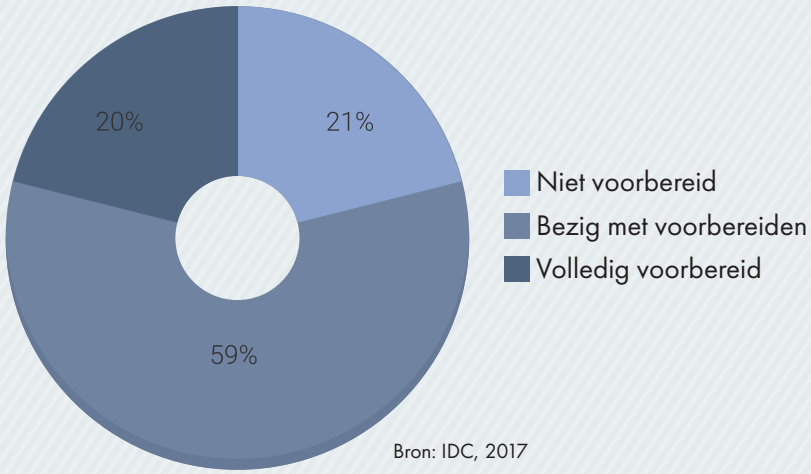
GDPR-compliant

Bent u zich bewust van de impact van de GDPR op uw organisatie?



Bron: IDC, 2017

In welke mate bent u voorbereid op de GDPR?



Bron: IDC, 2017

Behoort u ook tot het percentage dat nog midden in de voorbereiding zit of hiermee nog moet starten? Maak dan gebruik van het handige stappenplan op de volgende pagina.

Stappenplan

- [x] **Informatie**
  Laat u vooraf voldoende informeren zodat u bewust wordt wat de GDPR voor u betekent.

- [ ] **Verwerkingsregister**
  Maak eerst een register aan om alle mutaties van de persoonsgegevens in vast te leggen. Beschrijf per verwerking wat het doel was, wie verantwoordelijk is en welke preventieve beveiligingsmaatregelen zijn getroffen.

- [ ] **Categorisering van persoonsgegevens**
  Categoriseer de gevoeligheid van de persoonsgegevens en beoordeel de aanwezige risico's.

- [ ] **Beveiligingsmaatregelen**
  Implementeer technische middelen en organisatorische procedures ter waarborging van de goede beveiliging van verwerkte persoonsgegevens. Documenteer en beschrijf alle getroffen maatregelen. Monitor met behulp van een managementcyclus de gezondheid van de systemen en draag zorg voor het regelmatig uitvoeren van beveiligingsupdates.

- [ ] **Privacy Impact Assessment**
  Toets periodiek of de getroffen maatregelen nog in lijn zijn met de GDPR. Beoordeel of de risico's beheersbaar zijn en of de doelstellingen ook behaald kunnen worden met minder persoonsgegevens. Voer altijd een privacy impact assessment uit wanneer interne of externe omstandigheden wijzigen.

- [ ] **Privacy by Design**
  Zorg dat bij het verwerken van persoonsgegevens de criteria worden gehanteerd zoals eerder is vastgelegd.

- [ ] **Transparant**
  Informeer de betrokkenen over het proces en de maatregelen die zijn getroffen. Geef aan met welk doel u welke gegevens vraagt en op welke wijze u die verwerkt. Overweeg om privacy impact assessment rapportages te delen.

- [ ] **Data Protection Officer**
  Stel een Data Protection Officer (DPO) aan indien de criteria u daartoe verplichten. De DPO dient zich toegangelijk op te stellen naar de betrokkenen toe.

- [ ] **Detectie beveiligingsincidenten**
  Implementeer maatregelen om beveiligingsincidenten te detecteren zoals een 24/7 scan en monitoring applicatie. Dit beperkt tevens de gevolgen van een incident en zorgt voor documentatie.

- [ ] **Melden datalek bij autoriteiten**
  Richt een procedure in bij een situatie met een datalek. Voldoe op deze wijze aan de verplichting om een lek binnen 72 uur na detectie aan de Autoriteit Persoonsgegevens te melden. Zorg daarnaast voor documentatie van het betreffende datalek.

- [ ] **Melden datalek bij betrokkenen**
  Implementeer een procedure waarmee betrokkenen kunnen worden geïnformeerd in geval van een datalek met nadelige gevolgen.

P +31 (0)20 788 10 30 F +31 (0)20 788 10 40 E sales@networking4all.com W www.networking4all.com
PO Box 15320 1001 MH Amsterdam The Netherlands