onlinQ

Wat betekent de GDPR voor mijn bedrijf?

TOM VAN NUNEN
ONLINQ BEST

Onderwerpen

- Doel van GDPR
- Welke bedrijven hebben te maken met de GDPR?
- Basiselementen van de GDPR
- Wat zijn de gevolgen van het niet naleven van de nieuwe wet?
- Hoe bereid je jouw bedrijf voor op de GDPR?

Doel van de GDPR

Meer controle geven aan mensen

- Wbp was ‘achterhaald’
- Wetgeving nodig om gegevensbescherming te verbeteren
- Strengere handhavingsmaatregelen

Eenvoudige en duidelijke juridische omgeving

- Eén wetgeving voor de gehele EU

Welke bedrijven hebben te maken met de GDPR?

Welke bedrijven hebben te maken met de GDPR?

- GDPR geldt voor alle bedrijven die persoonsgegevens van Europese burgers verwerken.
- Deze bedrijven dienen een GDPR compliance programma te ontwikkelen.

Basiselementen van den GDPR

Basiselementen van de GDPR

- Transparant zijn over verwerking en gebruik van persoonsgegevens.
- Beperken van verwerking van persoonsgegevens tot specifieke, legitieme doeleinden.
- Beperken van verzameling en opslag van persoonsgegevens tot beoogd gebruik.
- In staat stellen van individuen om persoonsgegevens te corrigeren of om verwijdering te vragen.
- Beperken van de opslagduur van persoonsgegevens tot zo lang als nodig is voor het beoogd gebruik.
- Beveiligen van persoonsgegevens met geschikte beveiligingsmethoden.

Wat zijn de gevolgen van het niet naleven van de nieuwe wet?

Wat zijn de gevolgen van het niet naleven van de nieuwe wet?

- Flinke boetes van de Autoriteit Persoonsgegevens
- Artikel 58 van de GDPR bepaalt dat de AP boetes mag opleggen op basis van:
  - De aard, ernst en duur van de overtreding (bijvoorbeeld hoeveel mensen er zijn getroffen en hoeveel schade zij hebben geleden);
  - Of de overtreding een bewuste keuze is of door nalatigheid;
  - Het type persoonsgegevens dat betrokken is

Wat zijn de gevolgen van het niet naleven van de nieuwe wet?

- Boetecategorie I:
  - 2 procent van de omzet
  - Maximum van 10 miljoen
- Boetecategorie II:
  - 4 procent van de omzet
  - Maximum van 20 miljoen

Categorie I -> Eerste keer overtredingen

Categorie II -> Nalatigheid, herhaalde overtredingen of grove schendingen

Hoe bereid je jouw bedrijf voor op de GDPR?

Hoe bereid je jouw bedrijf voor op de GDPR

- Breng in kaart welke persoonsgegevens jouw bedrijf heeft
- Identificeer jouw rol in het gebruik van persoonsgegevens
- Ontwikkel een sterk beveiligingsprogramma
- Verwerk persoonsgegevens alleen bij toestemming van betrokkenen
- Bepaal of jouw bedrijf een Data Protection Officer nodig heeft
- Ontwikkel een beleid bij een datalek

Breng in kaart welke persoonsgegevens jouw bedrijf heeft

- Identificeer welke persoonsgegevens je hebt en hoe het is opgeslagen en verwerkt.
- Denk hierbij aan welke systemen deze persoonsgegevens zijn verzameld en opgeslagen.
- Identificeer waarom deze gegevens zijn verzameld, hoe ze zijn verwerkt en gedeeld en hoe lang ze bewaard worden.

Identificeer jouw rol in het gebruik van persoonsgegevens

- Ben je een data-controller of een data-processor?
  - Een data-controller stelt vast hoe en waarom persoonsgegevens zijn verwerkt.
    Bv. ieder commercieel bedrijf
  - Een data-processor verwerkt daadwerkelijk de persoonsgegevens
    Bv. een IT-bedrijf die de daadwerkelijk verwerkt.

Ontwikkel een sterk beveiligingsprogramma

- Databeveiliging vereist een sterk beveiligingsprogramma.
  - Beleid
  - Systemen
  - Technologieën

Verwerk persoonsgegevens alleen bij toestemming van betrokkenen

- Hoe worden persoonsgegevens verzameld?
- Heb je expliciet toestemming gekregen van de betrokkene?

Jouw bedrijf kan persoonsgegevens van een klant hebben gekregen om een product of dienst te leveren, maar dit betekent niet dat je ook toestemming hebt gekregen om over promoties te communiceren.

Voor elke specifieke activiteit moet je toestemming krijgen. De toestemming moet ook altijd weer ingetrokken kunnen worden.

Bepaal of jouw bedrijf een Data Protection Officer nodig heeft

- Advies: Maak een gekwalificeerd persoon verantwoordelijk voor het beveiligen van persoonsgegevens en GDPR compliance.
- Dit is verplicht in de volgende situaties:
  - Persoonsgegevens die worden beheerd of verwerkt door een overheidsorganisatie. Rechtbanken vormen een uitzondering op deze regel.
  - Bedrijven die regelmatig en systematisch op zeer grote schaal persoonsgegevens verwerken
  - Bedrijven die op grote schaal persoonsgegevens verwerken van bijzondere, vaak voor strafrechtelijke doeleinden bestemde informatie. Gegevens met betrekking tot misdaden en veroordelingen vallen hier ook onder!

Verwerk persoonsgegevens alleen bij toestemming van betrokkenen

- Hoe worden persoonsgegevens verzameld?
- Heb je expliciet toestemming gekregen van de betrokkene?

Jouw bedrijf kan persoonsgegevens van een klant hebben gekregen om een product of dienst te leveren, maar dit betekent niet dat je ook toestemming hebt gekregen om over promoties te communiceren.

Voor elke specifieke activiteit moet je toestemming krijgen. De toestemming moet ook altijd weer ingetrokken kunnen worden.

Ontwikkel een beleid bij een datalek

- Sinds 1 januari 2016 geldt de meldplicht datalekken.
- Bij een datalek in jouw bedrijf moet je binnen 72 uur melding maken bij de AP.
- De acties die in de eerste 24 uur ondernomen worden zijn cruciaal
- Wat dient in het beleid te staan?
  - De leden van het datalek team
  - De acties die ondernomen moeten worden als een werknemer een datalek vermeodt, ontdekt of rapporteert inclusief wanneer diegene het datalek team moet inschakelen;
  - De acties die ondernomen moeten worden door het response team

Wat is een datalek?

- Een datalek is een inbreuk op de beveiliging van persoonsgegevens
- Bij een datalek zijn de persoonsgegevens blootgelegd aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.
- *Voorbeelden:*
  - *Een kwijtgeraakt apparaat met persoonsgegevens,*
  - *Een inbraak in een databestand door een hacker of*
  - *Iemand die persoonsgegevens per ongeluk naar de verkeerde persoon verstuurt.*