Checklist GDPR-compliant in 6 stappen

Is mijn bedrijf GDPR compliant?

Toen de nieuwe GDPR-regelgeving eraan kwam, was zowat elk bedrijf er bewust mee bezig. Maar na 25 mei 2018 zijn de meeste inspanningen op een lager pitje gezet. En dat is jammer, want ons dataverbruik blijft stijgen en problemen met privacy halen regelmatig de krantenkoppen. GDPR vraagt om een continue inspanning. Hou deze lijst daarom bij en kijk ze regelmatig na.

1. Iedereen in mijn bedrijf kent de basisprincipes van GDPR en leeft ze na

Het steekt niet zo nauw, denkt u misschien. Maar dat klopt niet. GDPR raakt ons allemaal: werknemers, freelancers, leveranciers ... Iedereen die met persoonsgegevens in aanraking komt. En een probleem met GDPR kan vanuit een onverwachte hoek komen. Zorg daarom voor een vaste strategie en maak uw beleid duidelijk aan alle betrokkenen.

Medewerkers die met persoonsgegevens in contact komen, laat u best een GDPR-opleiding volgen. Meestal gaat dit om medewerkers van de afdelingen hr, marketing en klachten- en klantendienst.

TIP! Toon nieuwe werknemers deze video, dan zijn ze meteen mee.

Checklist GDPR-compliant in 6 stappen

2. Al mijn documenten die persoonsgegevens bevatten, zijn GDPR-compliant

- **Privacypolicy en privacystatements**

  Deze moeten de gegevens bevatten van de verwerkingsverantwoordelijke, de DPO, de rechtsgronden van de verwerking ...

  TIP! Nog niet helemaal klaar? Download onze handige checklist privacypolicy GDPR

- **Cookiepolicy**

  GDPR gaat ook om klare taal. In de GDPR staat letterlijk 'Voor iedere cookie die een bezoeker kan identificeren, moet hij of zij apart zijn toestemming geven.' Maak uw cookiebeleid dus zo helder mogelijk.

- **Contracten**

  Mijn contracten met werknemers, freelancers, leveranciers, klanten ... zijn bijgewerkt: opt-in-clausules, privacyclausule, algemene voorwaarden ...

3. Mijn interne procedures zijn afgestemd op de GDPR-richtlijnen

- Ik vind aanvragen van betrokkenen om hun gegevens in te kijken, te wissen, te verbeteren of om de verwerking te beperken, onmiddellijk terug.
- Ik respecteer hun recht op overdraagbaarheid van de gegevens.
- Ik weet hoe ik moet reageren op een datalek of bij een inbreuk op persoonsgegevens.
- Ik weet wanneer en hoe ik de Gegevensbeschermingsautoriteit en de betrokkenen moet verwittigen.
- Mijn opt-in-beleid is GDPR-compliant.
- Ik kan een DPIA (Data Protection Impact Assessment) uitvoeren en weet wanneer ik dit moet doen.
- Ik weet hoe ik moet reageren bij een controle of verzoek van de Gegevensbeschermingsautoriteit.
- Ik heb evaluatieprocedures voor IT-beveiliging, dataregisters en policies.
- Ik heb een privacyorganigram.
- Ik weet welke bevoegdheden alle rollen hebben.

4. Al mijn softwareproducten zijn beveiligd

- Niemand kan aanmeldgegevens hacken, stelen of per ongeluk zien.
- Alle wachtwoorden zijn gecodeerd zodat niemand ze kan zien, ook niet mijn ontwikkelaars op de supportafdeling.

Checklist GDPR-compliant in 6 stappen

5. Mijn persoonsgegevens zijn correct geïnventariseerd in een dataregister. Dat betekent dat ze volgende zaken bevatten:

- de naam en contactgevens van de verwerkings-verantwoordelijke en eventuele subverwerkers;
- de aard van de verwerkte gegevens, onderverdeeldd in categorieën;
- een onderverdeling 'gevoelige gegevens';
- waarom u de gegevens verwerkt en wat u er mee doet (doel en rechtsgrond);
- waar u de gegevens bewaart;
- of en aan wie u gegevens overdraagt;
- wie toegang heeft tot de gegevens en welke beschermingsmaatregelen zij treffen;
- tot wanneer u de gegevens gebruikt of bewaart, voor elke categorie;
- hoe u de gegevens beschermt.

TIP! Niet meer zeker wat persoonsgegevens precies zijn? Bekijken onze paper 'Persoonsgegevens GDPR'

6. Mijn GDPR-processen en -procedures staan op punt

- Ik reageer op elk verzoek van betrokkenen, binnen een maand.
- Ik documenteer datalekken, evalueer ze en volg ze op.

  Bij datalekken denken we vooral aan kwaad opzet zoals hacking, ransomware en diefstal. In werkelijkheid zijn datalekken meestal het gevolg van een menselijke fout: iemand verliest een usb-stick, publiceert per ongeluk persoonsgegevens op een onbeveiligde webpagina, het computersysteem crasht ...

- Ik evalueer voortdurend en systematisch de compliancy van mijn procedures, de IT-beveiliging en de contracten.

Wil u helemaal GDPR-proof zijn, zonder zorgen? Speel op zeker en neem een GDPR-omnium! →

V.U.: Paul De Ridder • Motstraat 30 • 2800 Mechelen