

GDPR STATEMENT



Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) of meestal **General Data Protection Regulation (GDPR)** in werking. Deze Europese Verordening legt een aantal strikte verplichtingen en regels op in het kader van de bescherming van persoonsgegevens en moet gezien worden als een verstrenging van de privacy regels waar nu reeds moet aan voldaan zijn.

In het kader van de samenwerkingsovereenkomst die onze onderneming heeft afgesloten met haar contacten treedt de onderneming in termen van GDPR op als **'verwerkingsverantwoordelijke' van persoonsgegevens.**

Overeenkomstig de toepasselijke reglementering in het kader van privacy en bescherming van persoonsgebonden gegevens, staat onze onderneming garant voor een kwalitatief niveau van gegevens- en databeveiliging, en dit door het nemen van alle noodzakelijke & redelijke technische en organisatorische maatregelen.

Hieronder vindt u alvast een niet-limitatieve opsomming van de vooropgestelde maatregelen in dit kader:

Op technisch-infrastructureel vlak:

- 1) Controle op de toegang van lokalen en bedrijfsruimten via beveiligd toegangsbeheer;
- 2) Fysieke beveiliging van alle computerlokalen en serverlokalen waar software en data zich bevinden. De concrete beveiliging omvat onder meer een beveiligd toegangsbeheer, koelsysteem, alarmsysteem, stroomonderbrekingsinstallatie en brandbeveiligingssysteem;
- 3) Controle van toegang tot gebruik van IT-installaties en processen;
- 4) Een meervoudig back-up proces dat toelaat om gegevens terug te zetten;
- 5) Afscherming van de toegang tot de verwerkte gegevens d.w.z. enkel toegang voor de personen die in het kader van de toevertrouwde opdracht toegang moeten hebben. Dit gebeurt via een geformaliseerd systeem van paswoorden en toegangsrechten op basis van rollen en verantwoordelijkheden;

- 6) Access management: enkel toegang tot persoonlijke gegevens voor personen die uit hoofde van hun functie en enkel voor dit doel toegang tot deze gegevens moeten hebben;
- 7) Een systeem van logische beveiliging op basis van een intern beheerde firewall en virus scanner;
- 8) Een geformaliseerd releasemanagement, change management, testing met scheiding van ontwikkelings-, acceptatie- en productieomgevingen;
- 9) Controle op de invoer, wijziging en schrapping van gegevens via een systeem van logging zodat achteraf kan vastgesteld worden wie welke wijzigingen heeft aangebracht in de software-applicaties;
- 10) Er werd een dataverwerkingsregister opgesteld met alle verwerkingsactiviteiten van persoonsgegevens op basis van het model van register dat door de Privacy Commissie werd ter beschikking gesteld;

Organisatorisch

- 11) Interne Privacy Policy van kracht met richtlijnen voor de medewerkers omtrent het in de praktijk omgaan met persoonsgegevens, zowel binnen de organisatie als naar klanten en derden toe. Daarbij zal de geheimhoudingsplicht en de bescherming van de persoonlijke levenssfeer zeer duidelijk voorop gesteld worden;
- 12) Informeren en sensibiliseren van alle interne medewerkers met betrekking tot de verstrengde regels opgelegd door GDPR via periodieke opleidingen en infosessies;

Juridisch

- 13) In het arbeidsreglement zijn bepalingen opgenomen met betrekking tot de geheimhouding en bescherming van de persoonlijke levenssfeer inzake gegevens die ons in het kader van onze opdracht werden toevertrouwd. Deze documenten worden bijgewerkt waar nodig om te voldoen aan GDPR vereisten;
- 14) Opmaak van een verwerkersovereenkomst te ondertekenen met de leveranciers / dienstverleners die volledig voldoet aan de vereisten vooropgesteld door GDPR;

Voor verdere vragen kan u steeds contact opnemen met:

Human Resources