AVG: technische en organisatorische maatregelen ter bescherming van persoonsgegevens

Technische maatregelen:

- Persoons- en organisatiegegevens worden opgeslagen in de database van webbased ERP software Webflow via een beveiligde verbinding. Gevoelige informatie (b.v. logingegevens) wordt versleuteld opgeslagen in de database. De software draait op een virtuele server in beveiligde datacenters in Nederland (Delft, Amsterdam) en wordt elke 4 uur geback-upt. Het datacenter bezit de volgende certificeringen:
    - ISO 9001
    - ISO 27001
    - ISO 14001
    - NEN 7510
    - PCI DSS
- Persoons- en organisatiegegevens worden tevens opgeslagen in bestanden op de beveiligde cloud storage My Secure Filesync. De bestanden worden opgeslagen in een beveiligd Nederlands datacenter in Amsterdam, zijn met 448-bit versleuteling beveiligd en worden dagelijks geback-upt. De lokaal opgeslagen gegevens kunnen worden vernietigd bij diefstal van het betreffende apparaat.
- Software (zoals browsers, virusscanners en operating systems) worden up-to-date gehouden middels periodieke controle en het (automatisch) uitvoeren van updates indien nodig.
- Technische kwetsbaarheden (patch management) worden periodiek gecontroleerd en (automatisch) direct opgelost waar nodig.
- Het kantoor is voorzien van een goedgekeurd toegangsslot en alarm.
- Pc's op kantoor zijn voorzien van adequate veilige wachtwoorden en antivirussoftware.
- In de router en op de PC's is een firewall aanwezig.

Organisatorische maatregelen:

- De verantwoordelijkheid voor informatiebeveiliging ligt bij de eigenaren. Er wordt op toe gezien dat medewerkers de gemaakte afspraken omtrent informatiebeveiliging naleven.
- Bestaande en nieuwe medewerkers worden bewuster gemaakt van het belang van informatiebeveiliging.
- Er zijn afspraken gemaakt over de plek waar persoons- en organisatiegegevens opgeslagen worden. Er wordt gestreefd naar het opslaan van persoons- en organisatiegegevens op 1 centrale plek.
- Er zijn procedures opgesteld om periodiek de genomen beveiligingsmaatregelen te testen, te beoordelen en te evalueren.
- Logbestanden worden regelmatig gecontroleerd.
- Voor de afhandeling van datalekken en beveiligingsincidenten is een protocol opgesteld.

- Er zijn geheimhoudings- en/of verwerkersovereenkomsten gesloten met personen en organisaties waarvoor dat van toepassing is.
- Er wordt regelmatig geëvalueerd of dezelfde doelen behaald kunnen worden met minder persoonsgegevens.
- Verleende toegang tot persoonsgegevens aan personen binnen de organisatie is tot een minimum beperkt.