Beveiligingsmaatregelen AVG

- De toegang tot data is beveiligd. Alleen gebruikers met een gebruikersnaam en een wachtwoord hebben toegang tot (delen van) de data;
- Wachtwoorden dienen geheim te worden gehouden;
- Op basis van rechten en rollen wordt geautomatiseerd invulling gegeven aan functiescheiding doordat via autorisaties functies worden toegekend aan onze kantoormedewerkers. Hierdoor kunnen registrerende-, bewarende- en beschikkende functies van elkaar gescheiden worden. Functiescheiding geldt zowel voor systeembeheerfuncties als voor het gebruik van de (administratieve) softwaresystemen;
- Er mag geen data worden opgeslagen op losse media zoals USB sticks, notebooks, tablet-pc's en smartphones.
- De toegang tot de computers is beveiligd met een toegangscode om te voorkomen dat derden (onbevoegd) toegang krijgen tot de data;
- (Geactiveerde) computers (ook laptops, smartphones en andere mobiele apparaten) dienen onder toezicht te blijven van de eigenaar en mogen niet (zonder beveiliging) onbeheerd achter gelaten worden (zoals in auto, trein, etc.);
- Data wordt opgeslagen op de centrale server. Het is niet toegestaan om relevante bestanden lokaal op de pc op te slaan mede in verband met het maken van back-ups en de toegankelijkheid tot de bestanden door andere medewerkers. Daarnaast ontstaat verlies van data bij een eventuele stroomuitval;
- Onze systemen zijn centraal beveiligd tegen virussen en spyware door middel van antivirussoftware, Anti-spywaresoftware en een firewall;
- Geautomatiseerde gegevensuitwisseling met derden is zodanig ingericht dat de rechtmatigheid ten aanzien van het verkrijgen van gegevens is gewaarborgd door middel van authenticatie en geautomatiseerde vastlegging van raadplegingen;
- Voor het beschikbaar houden van data hanteren wij een back-up procedure inclusief het periodiek testen van het terugzetten. Iedere nacht wordt een back-up gemaakt. De meest actuele back-up wordt buiten ons kantoor bewaard. Periodiek wordt door de interne automatiseringsverantwoordelijke het terugzetten van een back-up getest op een juiste werking ;
- De updates van besturingssystemen op zowel de pc's (alsmede notebooks, tablet-pc's en smartphones) als de server worden zo spoedig mogelijk geïnstalleerd zodra deze beschikbaar komen;
- Minimaal eenmaal per jaar wordt de bedrijfszekerheid van en de risico's rondom de kritieke systemen door de interne automatiseringsverantwoordelijke samen met de externe automatiseringspartner geëvalueerd.

- **Organisatorische beveiligingsmaatregelen**
- Clean desk policy;
- Laptop nooit achterlaten in de auto;
- Fysieke dossiers nooit achterlaten in de auto;
- Oude documenten op juiste manier vernietigen;
- Arbeidsovereenkomsten met geheimhoudingsverklaringen;
- Inlognaam en wachtwoord zijn persoonsgebonden en geven toegang tot de computersystemen;
- Het downloaden van software is niet toegestaan, tenzij vooraf (schriftelijke) toestemming is verleend door de directie;
- Gratis software mag niet worden gebruikt wanneer deze niet vanuit het kantoor beschikbaar is gesteld;
- Onbedoelde inbreuken op beveiliging, van binnenuit of van buitenaf, dienen onmiddellijk aan de operationeel manager te worden gemeld;
- In het algemeen geldt voor het gebruik van internet en e-mail op de werkplek dat dit bedoeld is ter ondersteuning van de dagelijkse werkzaamheden. Het is dan ook uitsluitend toegestaan internet- en emaildiensten onder werktijd voor zakelijke doeleinden te gebruiken. Buiten werktijd en tijdens pauzes is privégebruik uitsluitend toegestaan met toestemming van de directie; dit gebruik dient echter tot een minimum beperkt te blijven;
- Medewerkers worden op de hoogte gesteld van de inhoud van dit artikel en dienen dit te onderschrijven en verplichten zich hiernaar te handelen;
- Na ernstige niet-nakoming van de afspraken zal de directie een formele, schriftelijke waarschuwing aan betreffende medewerker geven;
- Wanneer na de formele waarschuwing nog steeds sprake is van niet-nakoming van de afspraken, volgt ontbinding van de arbeidsovereenkomst zonder vergoeding (BW art. 7: 685).
- Bij het niet nakomen van de afspraken voortvloeiende uit dit artikel, zullen door de directie disciplinaire maatregelen worden getroffen;