ANNEX 2:

Overzicht beveiligingsmaatregelen

Huidige annex bevat een overzicht van de beveiligingsmaatregelen die de Verwerker minstens in acht neemt om de Persoonsgegevens die hij verwerkt maximaal te beschermen.

De Verwerker neemt met name naar best vermogen alle redelijke, passende technische en organisatorische beveiligingsmaatregelen die ervoor zorgen dat de toevertrouwde Persoonsgegevens geen voorwerp zijn van verlies of van onrechtmatige verwerking waaronder toegang door onbevoegden.

Om vast te stellen welke de passende beveiligingsmaatregelen zijn, wordt een afweging gemaakt op basis van de risico's van de verwerking aan de hand van onder meer volgende criteria:

- Het soort Persoonsgegevens dat wordt verwerkt (gevoelig of niet gevoelig);
- De hoeveelheid Betrokkenen van wie gegevens worden verwerkt;
- Het doel waarvoor de Persoonsgegevens worden verwerkt;
- …

Overzicht technische beveiligingsmaatregelen:

- Het gebruik van een virusscan;
- Installatie van een firewall;
- Het hanteren van een paswoordpolicy nl. unieke logincodes en persoonlijk wachtwoord dat regelmatig wordt aangepast;
- Systematisch maken van beveiligde back-ups om te beschermen tegen dataverlies;
- Afscherming van fysieke toegang tot persoonsgegevens voor personen die hier uit hoofde van hun takenpakket geen toegang toe moeten hebben;
- Geen gebruik maken van onbeveiligde harde schijven;
- Gebruik maken van encryptietechnieken bij de opslag van persoonsgegevens;
- Fysieke toegangsbeveiliging tot lokalen waar persoonsgegevens worden verwerkt en bewaard *(bv. aan de hand van badges of beveiligingscodes)*;
- …

Overzicht organisatorische maatregelen:

- Het hanteren van een algemeen informatiebeleid voor personeel i.v.m. privacy;
- Het organiseren van periodieke trainingen & awareness voor het personeel omtrent het omgaan met persoonsgegevens;
- Het opstellen van interne procedures i.v.m. indienst en uitdienst van medewerkers die persoonsgegevens beheren;
- Het vastleggen van vertrouwelijkheidsclausules met medewerkers die persoonsgegevens beheren;
- Het opstellen van een interne policy en richtlijnen i.v.m. het vertrouwelijk omgaan met persoonsgegevens;
- Het opstellen van interne procedures in geval van incidenten (gegevenslek, …);
- Het toepassen van een persoonlijke registratie en identificatiesystemen voor het monitoren van toegang tot de gebouwen zodat onbevoegden geen toegang krijgen tot de lokalen van de onderneming;
- Het aanduiden van een verantwoordelijke voor informatiebeveiliging;

- Het op regelmatige tijdstippen plannen en uitvoeren van interne veiligheidscontroles en –audits;
- Het hanteren van een clean desk-policy binnen onderneming waarbij vertrouwelijke gegevens maximaal worden afgeschermd voor onbevoegde personen;
- Het gebruik van papierversnipperaars of andere middelen om vertrouwelijke gegevens desgevallend te vernietigen;
- Het toepassen van een vastgelegde procedure omtrent het verwijderen van persoonsgegevens die zich bevinden op afgedankte apparatuur en opslagmedia (bv. op laptops en smartphones) en op apparatuur die terug ingediend wordt door medewerkers die de onderneming verlaten;
- ….