BIJLAGE 1 TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN

Wesselman verklaart de volgende technische en/of organisatorische maatregelen te hebben getroffen om persoonsgegevens te beschermen:

1. Software partner AFAS en IT partner ArcusIT
Wesselman maakt gebruik van de software van AFAS en heeft als IT partner ArcusIT.
Beide partijen beschikken over certificeringen die garant staan voor voldoende huidige beveiligingsmaatregelen op gebied van informatiebeveiliging. ArcusIT en AFAS werken beide volgens de normenkaders van ISO/IEC 27001. Dit is de meest bekende standaard voor requirements voor informatiebeveiliging. En zijn daarmee passende maatregelen voor informatiebeveiliging conform de AVG. (ISO, sd) (ArcusIT, 2016) AFAS heeft de ISAE 3402 norm voor beheersing van de kwaliteit en veiligheid van AFAS-online en de MJA-3 norm waarbij wordt getest of de systemen kwetsbaar zijn voor aanvallen.

2. Technische beveiliging van de cloud-omgeving Wesselman
Toegang tot de cloud werkomgeving van Wesselman is afgeschermd middels Two-factor authenticatie. De online omgeving van de gebruikte AFAS software is zo ingericht dat deze enkel te benaderen is vanuit de Wesselman cloud-omgeving. Binnen de Wesselman cloud-omgeving wordt middels single-sign-on ingelogd in de AFAS applicatie.

3. Interne maatregelen betreffende de organisatorische beveiligingsmaatregelen
Binnen Wesselman wordt een streng lock-screen policy gehanteerd voor een goede afscherming van gevoelige data. Wordt actief aandacht besteed aan een goede bewustwording voor wat betreft het omgaan met gevoelige data bij haar medewerkers en wordt een streng wachtwoordbeleid gehanteerd. Tevens wordt de kring van functionarissen die toegang hebben tot bepaalde persoonsgegevens beperkt tot enkel de personen welke deze gegevens nodig hebben voor het uitoefenen van hun werkzaamheden. Daarnaast is er met de medewerkers een geheimhoudingsbeding opgesteld met daaraan gekoppelde boeteclausule. Binnen Wesselman zijn er protocollen en procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en wordt er toezicht gehouden op de naleving van de protocollen en weten regelgeving.

4. Netwerk, internet beveiliging en login
Wesselman werkt met een afgeschermde digitale omgeving, waarin al de netwerkactiviteiten middels login vastgelegd en gemonitord worden. Deze omgeving is beveiligd middels met firewalls en de benodigde virusscanners om optimale veiligheid te realiseren.

5. Backup's
Er worden dagelijks back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Hierbij wordt een retentie van 30 dagen gehanteerd. Deze back-ups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving.

6. Fysieke beveiliging
De locaties van Wesselman beschikken over een alarminstallatie waarbij zorggedragen is aan opvolging indien het alarm afgaat. Tevens bevinden de bedrijfsservers zich in afsluitbare ruimtes op beide locaties, zowel Eindhoven als Helmond.