Annex 2 Veiligheidseisen

De Verwerker is overeenkomstig de AVG verplicht passende technische- en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. De volgende maatregelen zijn door Verwerker genomen om hieraan invulling te geven bij het leveren van de Diensten aan Verantwoordelijke:

Thema: "beschikbaarheid"

1. Data staat opgeslagen op servers die in Nederland staan;
2. Systemen worden actief gemonitord op beschikbaarheid en performance waarbij minimaal naar het gebruik van disk, CPU, intern geheugen en bandbreedte wordt gekeken. Op de monitoring zijn proactieve notificaties ingericht die beheerders op de hoogte stellen indien er onregelmatigheden zijn.
3. Security patches, updates en vernieuwing van SSL certificaten worden met vaste regelmaat uitgevoerd.
4. Gebruikte software en onderliggende bibliotheken van derden mogen niet End Of Life zijn.
5. Bij het in gebruik nemen van nieuwe functionaliteit (een release) wordt met geautomatiseerde Feature tests de impact op bestaande functionaliteit gecontroleerd om fouten te voorkomen.

Thema: "integriteit":

1. Gebruikers en beheerders die toegang hebben tot de systemen waarin persoonsgegevens worden verwerkt hebben standaard niet meer rechten dan nodig (least privilege).
2. Actieve gebruikersaccounts worden periodiek gecontroleerd en waar nodig opgeschoond.
3. Er wordt minimaal een dagelijkse snapshot / back-up van de gehele infrastructuur vastgehouden zodat we bij systeem falen een recente back-up kunnen terugzetten. Deze systeemsnapshots worden minimaal 14 dagen bewaard.
4. Maatregelen tegen malware of virussen zijn waar nodig toegepast
5. Gelogd wordt: inlogactiviteit van gebruikers (gelukt en niet gelukt) en wijzigingen van persoonsgegevens.
6. Logging wordt periodiek gecontroleerd op onregelmatigheden.

Thema: "vertrouwelijkheid"

1. Toegang tot systemen kan alleen met een voor elke gebruiker unieke gebruikersnaam en wachtwoord;
2. Voor accounts met toegang tot persoonsgegevens wordt naast een gebruikersnaam en wachtwoord ook 2 Factor Authenticatie afgedwongen.
3. Wachtwoorden en persoonsgegevens worden versleuteld in de database opgeslagen.
4. Alle wijzigingen in de software verlopen via een ontwikkel, test / acceptatie en productieomgeving (OTP).
5. Transport tussen systemen vindt eveneens versleuteld (TLS) plaats.
6. Toegang tussen systemen en op poortniveau is op basis van whitelists (firewalls) ingericht.

Naast deze maatregelen verzorgt HDI de volgende periodieke controles:

1. Minimaal 1x per jaar verzorgt HDI de volgende controles:
    - Er wordt een loadtest uitgevoerd
    - Er wordt een security en pen-test uitgevoerd (OWASP Top 10 kwetsbaarheden)
    - Er wordt een recovery test uitgevoerd (terugzetten van een back-up)

HDI verwacht van Verwerker redelijke medewerking en ondersteuning bij het oplossen van bevindingen die uit deze tests naar voren komen. Kosten voor de medewerking zijn voor Verwerker, kosten voor het oplossen van eventuele bevindingen zijn voor rekening van Opdrachtgever.