

Bijlage J: security en privacy eisen.

Het is van belang dat de Oplossing volledig voldoet aan de AVG, BIO en specifiek privacy en informatiebeveiliging by design, echter is het essentieel dat de processen die vervolgens in het systeem worden gezet en waar het systeem voor wordt gebruikt óók voldoen aan de AVG en BIO en specifiek privacy en informatiebeveiliging by design.

Privacy

Bijgaand de aanvullingen aangaande de eisen voor privacy:

- "De Opdrachtnemer voldoet aan de AVG, minimaal:
 - Afschermen van gegevens, dat inhoudt dat persoonsgegevens worden afgeschermd voor het gebruik voor andere doelen dan de doelen waarvoor ze mogen worden gebruikt.
 - Corrigeerbaarheid: voor elke verwerking van persoonsgegevens is het mogelijk om de persoonsgegevens aan te passen of te vernietigen, indien de verwerking niet voldoet aan de eisen; bijvoorbeeld in geval van onjuiste informatie of als er geen noodzaak meer is om de informatie te bewaren.
 - Transparantie: over elke verwerking van de persoonsgegevens is de volgende informatie beschikbaar: de verantwoordelijken, de categorieën persoonsgegevens, categorieën van betrokkenen, categorieën van ontvangers, doelbinding, de wettelijke grondslag, de bewaartermijnen, de beveiligingsmaatregelen en de organisatorische en technische inrichting van verwerking van de persoonsgegevens."
- Het systeem voldoet aan de Baseline Informatiebeveiliging Nederlandse gemeenten/Overheid (BIO)
- De Opdrachtnemer kan aan de hand een Privacy Impact Assessment (PIA) aantonen dat hij aan de AVG voldoet
- Het systeem voorziet in een goede afscherming op basis van rolgebaseerde toegang, en voorziet in een log/audit-trail die tenminste gegevens van 1 jaar direct inzichtelijk moet hebben en ten minste gegevens van de afgelopen 5 jaar vanuit backup beschikbaar moet hebben.
- Het systeem kan op eenvoudige wijze systeemrapportages genereren over het gebruik van de applicatie ten behoeve van audit-doeleinden.
- De Opdrachtnemer draagt zorg voor de veiligheid van alle onderdelen van de applicatie en de onderliggende infrastructuur/componenten en zorgt dat altijd de actuele beveiligingspatches geïnstalleerd zijn.
- De opslag van gegevens vindt fysiek en encrypted plaats binnen de EER
- De externe gepubliceerde onderdelen van de applicatie voldoen aan de minimale eisen van de Europese standaard EN 301 549.
- De Opdrachtgever werkt op verzoek van de Opdrachtnemer mee aan het uitvoeren van een DPIA op het systeem en de processen.