

Programma van eisen: Eisen ten aanzien van privacy en de verwerking van persoonsgegevens

NR.	Algemene eisen
1	Oprachtnemer voert jaarlijks een audit, DPIA-audit of pentest uit en rapporteert over de resultaten ervan.
2	Oprachtnemer werkt kostenloos mee aan een driejaarlijkse herziening van de DPIA. Bij grote wijzigingen werkt opdrachtnemer kostenloos mee aan onderzoek om na te gaan of de DPIA moet worden herzien.
3	De applicatie biedt een optie om accounts volledig te verwijderen. Er is een heldere verwijdermethode omschreven. Ingevoerde data blijft behouden en wordt conform bewaartermijn na 5 jaar geanonimiseerd.
4	Marketing subscriptions staan standaard uit of kunnen eenvoudig handmatig worden uitgezet.
5	Er worden heldere afspraken gemaakt over datalekken en beveiligingsincidenten.
6	In verband met privacy dient het datamodel voor wat betreft persoonsgegevens genormaliseerd te zijn, zodat privacy gevoelige gegevens op slechts 1 plek worden opgeslagen. Spoorlijnen worden bij registratie gekoppeld aan de persoon, maar in de opgeslagen historie worden persoonsgegevens niet metagegevens.
7	De opdrachtnemer heeft aantoonbaar technische en organisatorische maatregelen getroffen ter bescherming van de persoonsgegevens, om te voldoen aan de AVG.

NR.	Specifieke eisen
1	Doelbinding: Oprachtnemer zal de toegang en de autorisaties die zijn verleend ten behoeve van de uitvoering van de dienst(en) enkel voor dat doeleinde gebruiken en niet voor enig ander doeleinde.
2	Privacyverklaring: De organisatie heeft een privacyverklaring waarin is beschreven op welke wijze persoonsgegevens worden verwerkt en hoe een betrokkene, zijn of haar rechten kan uitoefenen.
3	Dataminimalisatie: Oprachtnemer draagt er zorg voor dat bij de uitvoering van de werkzaamheden niet meer persoonsgegevens of andere gevoelige gegevens worden ingezien of anderszins verwerkt dan werkelijk noodzakelijk voor het correct uitvoeren van de opdracht.
4	Privacybeleid: De organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijken worden opgelost.
5	Privacyorganisatie: De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen, zijn door de organisatie vastgelegd en vastgesteld, inclusief die bij uitwisseling van persoonsgegevens tussen organisaties, zodat ook bij doorgifte van persoonsgegevens de privacybelangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.
6	Privacy-bewustzijn: De organisatie waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.
7	Formele vastlegging handelen verwerkingsverantwoordelijke: De organisatie heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereidt, een actuele VOG, een actuele verklaring terzake het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht.
8	Privacy in de levenscyclus: Vooraf aan het ontwerp van een gegevensverwerking en bij een verandering wordt een inschatting gemaakt van de privacy-risico's en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.
9	Register van verwerkingsactiviteiten: De verwerkingsverantwoordelijke(n) en de verwerker(s) hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de vereisten van de AVG.
10	Datalekken: De organisatie heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de stakeholders vastgesteld om ze te kunnen informeren.
11	Datalekken: Oprachtnemer meldt datalekken/incidenten onverwijld, maar binnen maximaal 24 uur na ontdekken aan Opdrachtgever, dat er een datalek/incident heeft plaatsgevonden waarbij persoonsgegevens van Opdrachtgever betrokken zijn.
12	Doelbinding op rolniveau: De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.
13	Toegang op taakniveau: Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
14	Logging en monitoring uitgeven toegangsrechten: De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.
15	Internationale doorgifte: Inschrijver kan een actuele DTIA overleggen waarin: - Minimaal wordt beschreven welke risico's en kwetsbaarheden ontstaan bij het doorgeven van de gegevens buiten de EER; - Welke maatregelen getroffen moeten worden om de bovengenoemde risico's en kwetsbaarheden te mitigeren; - Of is bereid deze DTIA binnen 3 maanden na gunning uit te (laten) voeren en zal binnen 6 maanden na gunning genoemde maatregelen implementeren. DPIA (data protection impact assessment): Inschrijver kan een actuele DPIA overleggen waarin wordt beschreven welke risico's er zijn voor het delen van de gegevens naar een land buiten de EER en welke maatregelen zijn getroffen om deze risico's te mitiëren.
16	Verwerkersovereenkomst: Oprachtnemer zal de bij deze aanbesteding bijgevoegde verwerkersovereenkomst ondertekenen en meewerken in het actueel houden hiervan. Een eventueel benoemde aansprakelijkheidsbeperking zal niet van toepassing zijn op deze verwerkersovereenkomst.