

Bijlage 16 - Eisen ten aanzien van Privacy, AVG, Informatiebeveiliging in aanvulling op hoofdstuk 14 en 18 uit Bijlage 2 – Samenwerkvisie en Programma van eisen behorend bij 230121REG

Privacy

De Drechtsteden gemeenten hanteren "privacy by design" voor applicaties en systemen waarmee persoonsgegevens verwerkt worden. Deze principes komen voort uit de geldende wetgeving (AVG), maar ook uit de intentie om als Drechtsteden de privacy van onze inwoners en medewerkers te respecteren en dit via onze systemen zo veel mogelijk te garanderen. Hiervoor is het noodzakelijk dat het systeem voldoet aan onze eisen en wensen en dat de leverancier met ons meedenkt over het zo goed mogelijk inrichten van het systeem.

Nr.	Eisen
1	De Algemene Verordening Persoonsgegevens (AVG) en UAVG uitgangspunt voor elke vorm van gegevensregistratie, -verwerking en –uitwisseling waarbij de inschrijver op een transparante en praktische manier invulling geeft aan de verplichtingen uit de AVG. Inschrijver voegt bij de inschrijving een bijlage toe waarin omschreven wordt hoe de Inschrijver omgaat met de verwerking van persoonsgegevens.
2	Inschrijver heeft de informatieprocessen ingericht op basis van de principes van privacy by design en privacy by default en kan dit aantonen.
3	Inschrijver heeft extra maatregelen getroffen om gebleken onvolkomenheden op het gebied van privacy- en informatiebeveiliging te herstellen.
4	Wanneer nieuwe wetgeving of gewijzigde inzichten door jurisprudentie zich voordoen, verzorgt inschrijver in overleg (kosteloos) aanpassingen in het systeem (privacy flexibiliteit)
5	Inschrijver heeft een Functionaris Gegevensbescherming of een Privacy Officer met wie snel en op transparante wijze contact kan worden gelegd voor privacy gerelateerde onderwerpen.
6	Inschrijver biedt, indien van toepassing, de mogelijkheid documenten separaat te versleutelen (bijvoorbeeld een extra beveiliging op persoonsdossiers).
7	Inschrijver heeft een "state of the art" autorisatiematrix inrichting / architectuur. "Rol based access management" op een "need to know/least privilege" basis.
8	In geval van een SaaS- of een gehoste Applicatie vindt de opslag van gegevens niet plaats buiten de Europese Economische Ruimte en niet binnen het Verenigd Koninkrijk.
9	De Drechtsteden sluit met Inschrijver, voorafgaand aan de dienstverlening, een schriftelijke overeenkomst met betrekking tot de bescherming en de verwerking van persoonsgegevens cf. artikel 28 lid 3 AVG. Daarbij wordt het model verwerkersovereenkomst van de Drechtsteden gehanteerd dat overeenkomstig is met het landelijke model van de VNG/IBD inclusief de Relevante GIBIT 2020 artikelen (indien van toepassing).
10	Inschrijver mag de door de Drechtsteden verzamelde persoonsgegevens slechts in uitdrukkelijke opdracht van de Drechtsteden verwerken. Alle verzamelde en verkregen data gedurende de looptijd van het contract blijven eigendom van Opdrachtgever.
11	Inschrijver verwerkt de persoonsgegevens niet verder voor eigen doeleinden en verstrekt de gegevens niet zonder expliciete en schriftelijke toestemming van de Drechtsteden aan derden.
12	Inschrijver mag bij het verwerken van de persoonsgegevens alleen groepsmaatschappijen en onderaannemers/subverwerkers inschakelen als een schriftelijke overeenkomst is gesloten waarin dezelfde verplichtingen zijn opgenomen als in het model verwerkersovereenkomst van de Drechtsteden en hiervoor toestemming is verkregen van opdrachtgever (verwerkingsverantwoordelijke).

13	Inschrijver heeft een proces ingericht om mee te werken in geval van verzoeken van betrokkenen om hun wettelijke rechten uit te voeren. Inschrijver maakt het in haar systemen mogelijk om hun gegevens in te zien en biedt mogelijkheden voor betrokkenen om hun overige rechten i.h.k.v. de AVG uit te oefenen. Hieronder valt tevens de mogelijkheid de verwerking te "beperken", m.a.w. te bevriezen, zoals in de AVG opgenomen.
14	Inschrijver biedt de mogelijkheid de velden in haar systemen (data library) eenvoudig te kunnen verwijderen of te anonimiseren.
15	Inschrijver heeft bewaartermijnen (op metadata) per categorie persoonsgegevens ingesteld met als gevolg dat de gegevens automatisch worden verwijderd na het verstrijken van deze bewaartermijnen.
16	Inschrijver maakt geen gebruik van productie data binnen de testomgeving of ondersteuningsomgeving.