



Bijlage 3A bij Programma van Eisen

Specificatie eisen van Privacy by Design en Privacy by Default

Privacy by Design

Privacy by Design houdt in dat privacy en gegevensbescherming vanaf het begin in het ontwerp en de ontwikkeling worden meegenomen. Opdrachtnemer moet aantonen dat het systeem en de processen voldoen aan de volgende principes:

1. Minimale gegevensverwerking

Het systeem mag alleen de strikt noodzakelijke persoonsgegevens verzamelen en verwerken.

Functionaliteiten moeten worden ontworpen om gegevens minimalisatie te ondersteunen, zoals het automatisch anonimiseren of pseudonimiseren van gegevens waar mogelijk.

2. Beveiliging vanaf de basis

Het systeem moet standaard versleuteling toepassen voor gegevensopslag en -transmissie.

Beveiligingsmaatregelen, zoals multi-factor authenticatie en logging van toegang, moeten al in de kern van het systeem geïntegreerd zijn.

3. Transparantie en controle

Gebruikers en beheerders moeten inzicht krijgen in hoe persoonsgegevens worden verwerkt en wie toegang heeft.

Er moeten instellingen zijn waarmee gebruikers privacy voorkeuren eenvoudig kunnen beheren, zoals toestemming voor gegevensverwerking.

4. Ingebouwde rechten voor betrokkenen

Het systeem moet functionaliteiten bieden waarmee gebruikers eenvoudig hun rechten onder de AVG kunnen uitoefenen (zoals inzage, correctie en verwijdering van gegevens).

Gegevens moeten op verzoek eenvoudig geëxporteerd of verwijderd kunnen worden.

Privacy by Default

Privacy by Default betekent dat het systeem standaard is ingesteld op maximale gegevensbescherming, zonder dat gebruikers of beheerders handmatig privacy-instellingen hoeven aan te passen. Opdrachtnemer moet ervoor zorgen dat:

1. Beperkte standaardinstellingen

Alleen de strikt noodzakelijke gegevens worden standaard verzameld en verwerkt.

Opties die extra gegevensverwerking vereisen (zoals tracking of profilering) moeten standaard zijn uitgeschakeld en alleen ingeschakeld worden met expliciete toestemming.

2. Beperkte toegangsrechten

Toegang tot persoonsgegevens is standaard beperkt tot alleen geautoriseerde gebruikers op basis van het need-to-know-principe.

Rollen en rechten moeten standaard zo zijn ingesteld dat medewerkers alleen toegang hebben tot gegevens die noodzakelijk zijn voor hun functie.

3. Beperkte bewaartermijnen

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk en moeten standaard automatisch worden verwijderd of geanonimiseerd na de wettelijke of overeengekomen termijn.

Het systeem moet automatische verwijderingsopties ondersteunen.

4. Veilige standaardinstellingen

Beveiligingsmaatregelen zoals encryptie, sterke wachtwoorden en tweefactorauthenticatie moeten standaard zijn ingeschakeld.

Logging en monitoring van toegang en wijzigingen in persoonsgegevens moeten standaard actief zijn