Annex Xb Wensen m.b.t. InformatieBeveiliging en Privacy (IBP)

Voor het nieuw PIS (personeelsinformatiesysteem), of feitelijk elke applicatie/systeem dat persoonsgegevens verwerkt, zijn een aantal min of meer generieke IBP wensen aan de orde. Hieronder die generieke zaken die voor het PIS van het GLU ook meegenomen dienen te worden.

Criterium	Ja/Nee	Toelichting in hoeverre wel en niet.
De dienst/toepassing is ontwikkeld conform privacy by design, en ingericht conform privacy by default (artikel 25 van de AVG).		
Er zijn passende technische en organisatorische beveiligingsmaatregelen genomen voor de te verwerken per-soonsgegevens (artikel 32 van de AVG).		
De leverende organisatie is ISO 27001/27002 (of vergelijkbaar) gecertificeerd.		
Van de leverancier wordt verwacht dat haar betrokken werknemers een geheim-houdingsverklaring hebben getekend		
Opslag & transport van (persoons) gegevens vindt versleuteld plaats en wordt beheerd door de leverancier.		
Er is een DPIA uitgevoerd op de dienst/toepassing		
De aanbevelingen uit de uitgevoerde DPIA zijn opgepakt		
De uitgevoerde DPIA wordt ter beschikking gesteld aan het GLU		
Opslag en verwerking vindt in de EER plaats		
Geautomatiseerd schonen op basis van bewaartermijnen persoonsgegevens is mogelijk		
MFA is mogelijk, aansluiting bij Microsoft Azure is een optie.		
Autorisatiestructuur is rol gebaseerd en in te richten door het GLU		
In de ontwikkel-, test- en acceptatie-omgeving staan geen herleidbare persoonsgegevens		