

Bijlage A8 Beveiligingseisen webportal

Onderdeel	beschrijving
beveiliging	Authenticatie voor medewerkers van de Opdrachtgever dient te verlopen via twee-factor-authenticatie en bij voorkeur via de Entra ID van Opdrachtgever. (SSO)
	Toegang tot de kritieke onderdelen van de applicatie en data is beperkt tot de medewerkers van opdrachtnemer, die deze onderdelen onderhouden en/of installeren. Toegang tot de kritieke onderdelen van de applicatie is dwingend geregeld via een autorisatie op gebruikersnaam en kent strenge regels.
	De opdrachtnemer en eventuele hostingpartij is ISO 27001 gecertificeerd. Als bewijs een kopie van een recent behaald certificaat en de verklaring van toepasselijkheid meesturen. (max. 1 jaar oud)
	Applicatie dwingt HTTPS af door middel van HTTP Strict Transport Security (HSTS, RFC 6797).
	Opdrachtnemer dient bij beveiligingsincidenten noodzakelijke maatregelen nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. Het beveiligingsincident, alsmede alle getroffen maatregelen, worden aan de Opdrachtgever gerapporteerd.
	Opdrachtnemer voldoet aan de ICT-beveiligingsrichtlijnen voor Webapplicaties van het NCSC (in de toelichting aangeven hoe dit in- of extern wordt getoetst)
data	De opslag van data (productie en backup) vindt plaats binnen de Europese Economische Ruimte.
	Alle gegevens zijn en blijven te allen tijde eigendom van opdrachtgever en mogen door opdrachtnemer niet voor andere doeleinden worden gebruikt.
	Backups worden periodiek uitgevoerd.
gebruiksvriendelijkheid	De applicatie is geschikt voor verschillende soorten apparaten (laptop, tablet) en schaal, met uitzondering van beheerfuncties, mee met de afmetingen van een scherm van mobile devices tot tabletniveau, zonder in te leveren op leesbaarheid van tekst of bruikbaarheid van de gebruikersinterface (responsive design).