

Eisen Privacy en Informatie beveiliging

De Serviceorganisatie hanteert "privacy by design" voor applicaties en systemen waarmee persoonsgegevens verwerkt worden. Deze principes komen voort uit de geldende wetgeving (AVG), maar ook de intentie om als Serviceorganisatie 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 mee denkt over het zo goed mogelijk inrichten van het systeem, zodat het voldoet aan een hoge standaard op het gebied van privacy. De Serviceorganisatie stelt de volgende aanvullende eisen op gebied van Privacy:

Privacy eisen

De Algemene Verordening Persoonsgegevens (AVG) is 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 heeft de informatieprocessen ingericht op basis van de principes van privacy by design en privacy by default.
Inschrijver heeft extra maatregelen getroffen om gebleken onvolkomenheden op het gebied van privacy- en informatiebeveiliging te herstellen.
Wanneer nieuwe wetgeving of gewijzigde inzichten door jurisprudentie zich voordoen, verzorgt inschrijver in overleg (kosteloos) aanpassingen in het systeem (privacy flexibiliteit)
Inschrijver heeft een Functionaris Gegevensbescherming of een Privacy Officer met wie snel en op transparante wijze contact kan worden gelegd voor privacy gerelateerde onderwerpen.
Inschrijver heeft een "state of the art" autorisatiematrix inrichting / architectuur. " Rol based access management" op een "need to know/least privilege basis.
In geval van een SaaS- of een gehoste Applicatie vindt de opslag van gegevens plaats binnen de Europese Economische Ruimte.
Inschrijver verstrekt de gegevens niet zonder expliciete en schriftelijke toestemming van de Serviceorganisatie aan derden.
Inschrijver mag de door de Serviceorganisatie verzamelde persoonsgegevens slechts in uitdrukkelijke opdracht van de Serviceorganisatie verwerken en mag de persoonsgegevens niet verder verwerken voor eigen doeleinden.
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 Serviceorganisatie en hiervoor toestemming is verkregen van opdrachtgever (verwerkingsverantwoordelijke)
Inschrijver heeft bewaartermijnen (op metadata) per categorie persoonsgegeven ingesteld met als gevolg dat de gegevens automatisch worden verwijderd na het verstrijken van deze bewaartermijnen.

Inschrijver maakt geen gebruik van productie data binnen de testomgeving of ondersteuningsomgeving.

Informatiebeveiliging eisen

De Serviceorganisatie hecht veel waarde aan het juist en veilig opslaan van alle gegevens die door haar verwerkt worden. De Serviceorganisatie stelt de volgende aanvullende eisen op gebied van Informatiebeveiliging:

De infrastructuur en de organisatie van Inschrijver zijn adequaat beveiligd volgens ISO/IEC 27001 (of gelijkwaardig) en voldoen aan de voorwaarden genoemd in de Algemene verordening Gegevensbescherming (AVG);
Inschrijver stelt jaarlijks een Third Party Mededeling (TPM-verklaring) conform de eisen vanuit ISO/IEC 27001 (of gelijkwaardig);
Er wordt een toereikend recovery proces ingericht waar back-up en restore onderdeel van uit maken;
Er moet op jaarlijkse basis worden aangetoond dat het terugzetten (restore) van de backups (volledige Oplossing) succesvol verloopt, dit uiteraard in een tijdelijk daarvoor ingerichte restore omgeving, dus niet direct in Test-/ of Productie omgevingen;
De jaarlijkse TPM moet tenminste inzicht geven in hoeverre onderstaande procedures worden toegepast, op basis van opzet, bestaan en werking. - Assetmanagement - Back-up en Restore - Business Continuïteitsmanagement - Risicomanagement - Changemanagement - Autorisatie en toegangsprocedure - Logging en Monitoring - Incidentmanagement en response - Malware, patching, hardening, versleuteling procedures.
Het eigendom van de data ligt te allen tijde bij de Serviceorganisatie.
Inschrijver zal na gunning een incident response procesketen met de Serviceorganisatie inrichten en testen.
Het eigendom van tussentijds gemaakte back-ups (zowel op file- als ook op blocklevel) ligt te allen tijde bij de Serviceorganisatie.
Inschrijver draagt er zorg voor, dat mbt de omgeving waarin de data binnen de applicatie worden verwerkt, passende technische en organisatorische maatregelen zijn opgenomen om te kunnen voldoen aan de wettelijke eisen waaraan de Serviceorganisatie moet voldoen. Hiervoor gelden BIO / BIG / BIR / AVG / GIBIT.
De leverancier garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-upmedia) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. worden vervangen. Niet meer gebruikte gegevensdragers worden op een gecertificeerde wijze geschoond.

Bij datacommunicatie voor bestandsuitwisseling en voor de user interface wordt gebruik gemaakt van SSL versie 3 (Secure Sockets Layer) en cliënt- en servercertificaat technologie User -> SaaS SSLv3 en enkelvoudig geldig certificaat.LAN <--> SaaS: Tweezijdig authenticatie middels certificaten.
De medewerker van de leverancier heeft in het systeem alleen toegang tot de aan hem geautoriseerde functies en gegevens. Leverancier kan dit op verzoek aantonen.
Er is een totaaloverzicht beschikbaar van alle autorisaties van zowel de leverancier als de Serviceorganisatie.
IT voorzieningen en apparatuur bij de leverancier zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's
Systeemsoftware die bij de leverancier in gebruik is, wordt up-to-date gehouden.
Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig worden onmiddellijk gemeld aan en besproken met de Serviceorganisatie.
De leverancier verleent medewerking aan het uitoefenen van controle door of namens de Serviceorganisatie op bewaring en gebruik van gegevens en dat hij zijn verplichting tot adequate beveiliging nakomt. Een bezwaar van de leverancier tegen een door de Serviceorganisatie uit te voeren audit is niet acceptabel.
Inschrijver is verplicht de persoonsgegevens adequaat te beveiligen volgens de daarvoor van toepassing zijnde dataclassificatie. Inschrijver maakt expliciet welke beveiligingsmaatregelen met betrekking tot de door de Serviceorganisatie verzamelde persoonsgegevens worden genomen. Bij de beveiligingsmaatregelen moet worden gedacht aan de eisen die hieronder onder Informatieveiligheid zijn omschreven. Tevens moet een actuele en volledige beschrijving van het gehanteerde beveiligingsbeleid beschikbaar zijn voor de Serviceorganisatie.
De persoonsgegevens moeten encrypted worden opgeslagen conform ISO 27001/BIO. Het encrypten in het lifecycleproces van data gebeurt gedurende: - Creatie van data - Storage van data - Use van data - Share(delen)van data - Archive van data - Destroy van data
Inschrijver heeft een proces ingericht om beveiligingsincidenten en datalekken te constateren en onverwijld te melden aan de Serviceorganisatie en leeft deze na. Inschrijver heeft een gedetailleerd logboek van de beveiligingsincidenten en de maatregelen die op de beveiligingsincidenten zijn genomen. Serviceorganisatie mag dat inzien, wanneer zij daarom vraagt.
De Serviceorganisatie heeft een 'right to audit'