Bijlage 1B. Eisen Privacy en Informatiebeveiliging (PIV)

In aanvulling op de hieronder genoemde eisen bevat de laatste paragraaf de door gemeente Hoeksche Waard gehanteerde principes m.b.t. Privacy by design.

Nummer	Omschrijving
PIV.E1	Partijen garanderen te voldoen aan het vigerende privacybeleid en informatiebeveiligingsbeleid van gemeente Hoeksche Waard, en de Componentarchitectuur Authenticatie & autorisatie en Beveiliging en NCSC-ICT-Deel1&2-beveiligingsrichtlijn webapplicaties. Partijen zorgen ook voor passende technische en organisatorische maatregelen om vertrouwelijkheid en integriteit van (ICT-) systemen en informatie te waarborgen conform het voornoemde beleid. Dit beleid is van toepassing op alle ketenpartners (in welke hoedanigheid dan ook) en (sub-) verwerkers.
PIV.E2	Opdrachtnemer zorgt ervoor dat (meta)data van de Aanbestedende Dienst strikt gescheiden zijn van (meta)data van andere klanten van Inschrijver.
PIV.E3	Opdrachtnemer mag geen (meta)data van de Aanbestedende Dienst verwerken voor eigen doeleinden.
PIV.E4	Opdrachtnemer zorgt ervoor dat m.b.t. de omgeving waarin de data binnen de Opdracht worden verwerkt, passende technische en organisatorische maatregelen zijn genomen om te kunnen voldoen aan de wettelijke eisen waaraan de Aanbestedende Dienst moet voldoen. Hiervoor geldt de BIO en ook alle toekomstige wettelijke vereisten.
PIV.E5	Opdrachtgever is aan te merken als Verwerkingsverantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming (AVG). Opdrachtnemer is aan te merken als Verwerker in de zin van de Algemene Verordening Gegevensbescherming (AVG). Opdrachtnemer gebruikt de door Opdrachtgever verstrekte en in het kader van de (uitvoering van de) Overeenkomst ontvangen – al dan niet bijzondere – persoonsgegevens slechts voor het verrichten van de Prestatie zoals omschreven en vastgelegd in de Overeenkomst. Deze persoonsgegevens gebruikt Inschrijver niet voor andere doeleinden, al dan niet commercieel, dan beschreven in de opdrachten voor het verrichten van de Opdracht, evenmin voor eigen (verdere dan wel door-) ontwikkeling van producten, diensten en/of prestaties. De betrokken persoonsgegevens mogen niet (verder) worden verwerkt, verstrekt, uitgewisseld en gedeeld met derden, tenzij door Opdrachtgever op schriftelijk verzoek van Inschrijver daartoe uitdrukkelijke voorafgaande schriftelijke toestemming is gegeven.
PIV.E6	Opdrachtnemer garandeert compliant te zijn aan geldende en van toepassing zijnde landelijke en Europese wet- en regelgeving (en internationale) standaarden en normen voor gegevensbescherming en informatiebeveiliging.
PIV.E7	Bij gebruik van (sub)verwerkers / onderaannemers gelden dezelfde beveiligingseisen als voor de Opdrachtnemer. De Inschrijver is verantwoordelijk voor de borging bij de (sub)verwerkers / onderaannemer van de gemaakte afspraken.
PIV.E8	Alle gegevens (data) zijn en blijven te allen tijde eigendom van de Aanbestedende Dienst ook na beëindiging van de overeenkomst, en mogen door Inschrijver niet voor andere doeleinden worden

	gebruikt. De Aanbestedende Dienst kan deze gegevens op elk moment opvragen, waarna Inschrijver deze onmiddellijk beschikbaar zal stellen.
PIV.E9	Persoonsgegevens die in dit kader verwerkt worden, worden verwerkt en opgeslagen in één van de volgende landen (dit geldt tevens voor door Inschrijver ingeschakelde derde partijen): binnen de EU plus Noorwegen, Liechtenstein, IJsland (E.E.R), of in een ander land, mits aldaar passend privacybeschermingsniveau is gewaarborgd van een vergelijkbaar niveau als dat van de EU.
PIV.E10	Opdrachtnemer garandeert dat relevante wetswijzigingen worden opgevolgd en deze wijzigingen op functioneel, beveiligings- en/of technisch niveau per ingangsdatum effectief zijn en blijven gedurende de looptijd van de Overeenkomst in de betreffende (ICT-) systemen. In het geval er dergelijke wijzigingen worden doorgevoerd zullen Partijen elkaar daarover voorafgaand schriftelijk informeren.
PIV.E11	De Opdrachtnemer is verplicht per omgaande beveiligingsincidenten te melden bij de in de verwerkersovereenkomst aangegeven contactpersoon van Opdrachtgever. Potentiële datalekken dienen binnen 24 uur na ontdekking aan Opdrachtgever gemeld te worden. Hierbij wordt door Opdrachtnemer alle relevante informatie verstrekt aan Opdrachtgever. Op verzoek van Opdrachtgever worden logging gegevens en rapportages over informatiebeveiliging geleverd door Opdrachtnemer.
PIV.E12	Opdrachtnemer is verplicht mee te werken aan (IT)audits van Opdrachtgever. De Opdrachtgever behoudt de mogelijkheid om zelf audits uit te (laten) voeren.
PIV.E13	De Opdracht stelt Opdrachtgever in staat om te voldoen aan de bepalingen uit de Archiefwet.
PIV.E14	Bij beëindiging van de contractrelatie zal Opdrachtnemer kosteloos alle gegevens in een gangbaar en bruikbaar format zorgvuldig, tijdig en volledig wederom beschikbaar stellen aan de Opdrachtgever dan wel, na schriftelijke toestemming van Opdrachtgever, aan een opvolgende dienstverlener. Ook na beëindiging van de overeenkomst/werkzaamheden zal Opdrachtnemer eventuele kennis van, en gegevens over, personeelsleden en andere bedrijfsgegevens als strikt vertrouwelijk blijven beschouwen en niet aan derden verstrekken tenzij daartoe een wettelijke verplichting bestaat. Na beëindiging van de overeenkomst dient Opdrachtnemer, na overleg, de gegevens van de Opdrachtgever in haar eigen bedrijfshuishouding te vernietigen binnen de daarvoor geldende wettelijke kaders.

Privacy by design – principes

1. Dataverzameling: het proces van verzamelen van informatie ten behoeve van een bepaald doel. Privacy by design ten aanzien van dataverzameling houdt in:

1.1 Data minimalisatie: Er mogen niet meer persoonsgegevens verzameld worden dan strikt noodzakelijk voor het doel. Als persoonsgegevens worden verzameld, dient per element bepaald te worden of deze daadwerkelijk noodzakelijk zijn om het doel te behalen (Artikel 6 AVG).

1.2 Classificatie: Alle persoonsgegevens dienen correct te zijn geclassificeerd conform richtlijnen binnen de Gemeente Hoeksche Waard.

1.3 Wettelijke grondslag: Gegevensverzameling dient plaats te vinden op een wettelijke grondslag dienovereenkomstig AVG (Artikel 6 AVG).

1.4 Doelbinding: Werknemers en inwoners dienen op de hoogte te worden gesteld voor het verzamelen van persoonsgegevens ten behoeve van een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. De persoonsgegevens mogen uitsluitend voor dit doel gebruikt worden \

(Artikel 6 AVG).

1.5 Data herkomst: Het is duidelijk hoe persoonsgegevens zijn verzameld. Dit kan bijvoorbeeld middels een enquête, onderzoek, extractie uit interne bronsystemen, aanlevering van derde partijen, etc.

2. Dataverwerking: het verwerken en opslaan van gegevens zodat een snelle oproep mogelijk is. Privacy by design ten aanzien van dataverwerking houdt in:

2.1 Data kwaliteit: Persoonsgegevens moeten accuraat, compleet en actueel zijn. Dit houdt in dat de functionele waarde van een variabele bij bron (input) exact overeenkomt met de waarde in de output.

2.2 Inzage: Werknemers en inwoners hebben recht op inzage in hun persoonsgegevens. Systemen dienen dusdanig te zijn ingericht dat dit makkelijk opvraagbaar is (Artikel 15 AVG).

2.3 Rectificatie: Werknemers en inwoners hebben het recht op rectificatie indien er onjuiste persoonsgegevens zijn verwerkt (Artikel 16 AVG).

2.4 Verwerking minimalisatie: Werknemers en inwoners moeten bezwaar kunnen maken tegen de verdere verwerking van persoonsgegevens. Bijvoorbeeld indien onjuiste persoonsgegevens worden verwerkt (Artikel 18 AVG).

2.5 Doelbinding: Persoonsgegevens mogen enkel gebruikt worden ten behoeve van het doel waarvoor betreffende burger of werknemer toestemming heeft gegeven.

2.6 Recht op vergetelheid: Werknemers en inwoners moeten, indien een andere wetgeving dit niet tegenspreekt, een verzoek kunnen indienen tot verwijderen van de persoonsgegevens (Artikel 17 AVG).

3. Data beveiliging: b bescherming van gegevens tegen risico's van gegevensverlies of het in onbevoegde handen terechtkomen van persoonsgegevens en het zich daaruit voortvloeiende, onbevoegde gebruik of misbruik ervan. Privacy by design ten aanzien van data beveiliging houdt in:

3.1 Toegang (minimalisatie): Van de persoonsgegevens dient duidelijk te zijn wie toegang heeft en waarom. Richtlijn is toegang minimalisatie. Enkel voor wie toegang noodzakelijk is om het doel te behalen, krijgt toegang. Indien de onderliggende database van het systeem een OTAP straat bevat, dient per omgeving inzichtelijk te zijn wie toegang heeft. (Kortom autorisatiematrix per O-T-A-P).

3.2 Autorisatiebeheer: Het is duidelijk wie verantwoordelijk is voor autorisatie beheer en wat de procedure is voor aanvragen, wijzigen en verwijderen van rechten.

3.3 Encryptie: Persoonsgegevens noodzakelijk voor de business case, maar dusdanig gevoelig dat inzage of toegang niet gewenst is, dienen ge-encrypt te worden middels anonimisatie of pseudonimisatie.

3.4 Datalek procedures: Indien een datalek zich voordoet, dient duidelijk te zijn wie welke actie moet uitvoeren. Dit omvat de meldplicht en procedures binnen Gemeente Hoeksche Waard voor een onderzoek naar de oorzaak van de betreffende datalek.

3.5 Logging & monitoring: Detectie van ongeautoriseerde toegangspogingen dient correct te zijn ingericht.

4. Data retentie: opslaan en behouden (voor een bepaalde duur) van persoonsgegevens. Privacy by design ten aanzien van data retentie houdt in:

4.1 Data opslag: Het is duidelijk waar de persoonsgegevens zich bevinden. Dit kan zijn bijvoorbeeld in de Cloud, interne servers, externe servers, etc.

4.2 Bewaartermijn: Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor het gerechtvaardigd doel. Normaliter is de bewaartermijn tijdens de start van het project bepaald, echter wetgeving is aan verandering onderhevig en dient nauwlettend in de gaten gehouden te worden. De persoon van wie de gegevens zijn, dient ook geïnformeerd te worden over de bewaartermijn.

4.3 Verwijder procedure: Vooraf is bepaald of verwijdering handmatig of automatisch plaatsvindt. Het verwijderen van de persoonsgegevens, bijvoorbeeld na afloop contract, dient dusdanig plaats te vinden dat hiervan bewijs kan worden aangeleverd. Indien relevant dient dit tevens opgenomen te worden in het contract met partij waarmee persoonsgegevens worden uitgewisseld.