Bijlage E CKTO IB&P eisen

4. Generieke eisen ten aanzien van Privacy (P)

De AVG beschermt de grondrechten en de fundamentele vrijheden van levende natuurlijke personen en met name hun recht op bescherming van persoonsgegevens. In dit hoofdstuk worden niet de eisen herhaald die al zijn beschreven in de voorgaande hoofdstukken. Het geleverde dient additioneel op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-4.1	De geleverde oplossing dient gedurende de gehele looptijd van de overeenkomst te voldoen aan voor de SVB van toepassing zijnde wet- en regelgeving, waaronder maar niet beperkt tot de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).
IBPD-4.2	n.v.t.
IBPD-4.3	De Opdrachtnemer informeert de SVB ter beoordeling over hoe binnen de aangeboden oplossing invulling is gegeven aan de basisprincipes '***Privacy by Design',*** '***Privacy by Default*', '*Data Protection by Design***', '***Data Protection by Default***' en '***Data (collection and processing) minimalization***'.
IBPD-4.4	De geleverde oplossing dient mogelijkheden te bieden om te allen tijde te voldoen aan verzoeken in het kader van de rechten van betrokkenen.
IBPD-4.5	De geleverde oplossing dient mogelijkheden te bieden om aan personen gerelateerde gegevenselementen die niet of niet meer noodzakelijk zijn voor (latere) verwerkingen of waarvoor geen doelbinding / rechtsgrond meer aanwezig is te verwijderen.
IBPD-4.6	De geleverde oplossing dient mogelijkheden te bieden om aan de data gerelateerde retentie-policies zelfstandig in te regelen of in te laten regelen.
IBPA-4.7	De geleverde oplossing dient uitsluitend persoonsgegevens te verwerken, te transporteren en op te slaan binnen de Europese Economische Ruimte (EER). Tevens dienen de eventuele (privacy) restrisico's tot binnen de Risk Tolerance van de SVB gereduceerd te zijn. Dit geldt ook voor eventuele back-ups.
IBPA-4.8	Het Beheer en/of de Support van de geleverde oplossing dient bij voorkeur te gebeuren binnen de Europese Economische Ruimte (EER) of wordt geleverd van buiten de EER op basis van een geldig adequaatheidsbesluit of passende waarborgen zoals goedgekeurde en geldige binding corporate rules (BCR's), modelcontracten (standard contractual clauses (SCC's)) en een uitgevoerde Data Transfer Impact Assessment (DTIA), goedgekeurde gedragscode of certificeringsmechanisme.
IBPA-4.9	In de geleverde oplossing dient bij de verwerking van persoonsgegevens, zonder de uitdrukkelijke schriftelijke voorafgaande toestemming van de SVB, geen gebruik te worden gemaakt van subverwerkers. Dit geldt ook voor subverwerker-mutaties. *Met subverwerker wordt het volgende bedoeld:*

	"Organisaties kunnen de verwerking van persoonsgegevens uitbesteden aan een andere partij. Dit wordt de verwerker genoemd. Als deze verwerker de verwerking ook weer uitbesteedt aan een andere partij, dan is die partij de subverwerker."
IBPB-4.10	Opdrachtnemer dient een geïmplementeerd privacybeleid te hebben met daarin de doelstellingen, rollen en verantwoordelijkheden met betrekking tot privacy welke in overstemming zijn met op de SVB van toepassing zijnde wet- en regelgeving en in lijn met algemeen geaccepteerde privacy principes.
IBPB-4.11	Voorafgaand aan in productie name van de geleverde oplossing dient een verwerkersovereenkomst van de SVB afgesloten te zijn tussen de SVB als verwerkingsverantwoordelijke en de Opdrachtnemer als verwerker indien er persoonsgegevens worden verwerkt door de Opdrachtnemer.
IBPB-4.12	Opdrachtnemer dient de van de SVB ontvangen persoonsgegevens uitsluitend op basis van schriftelijke instructies van de SVB te verwerken voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die partijen zijn overeenkomen.
IBPA-4.13	Opdrachtnemer dient bij beëindiging van de dienstverlening de voor de SVB verwerkte persoonsgegevens te retourneren dan wel op verzoek van de SVB te vernietigen, tenzij er sprake is van een wettelijke bewaarplicht.
IBPB-4.14	Opdrachtnemer dient een proces te hebben en te hebben geïmplementeerd om datalekken onverwijld, maar uiterlijk binnen 24 uur, aan de SVB te melden.
IBPB-4.15	Opdrachtnemer dient de SVB op verzoek te allen tijde te ondersteunen bij het afhandelen van verzoeken van betrokkenen ter uitoefening van hun rechten en/of de opvolging of afhandeling van datalekken.
IBPB-4.16	Opdrachtnemer dient de SVB onverwijld, maar uiterlijk binnen 24 uur, over verzoeken tot aanlevering van (persoons)gegevens door buitenlandse inlichtingen- en opsporingsdiensten in het kader van de geleverde dienstverlening te informeren. Tenzij wetgeving dit niet toestaat.

6 Specifieke eisen aan de oplossing

In dit hoofdstuk worden niet de generieke eisen herhaald zoals beschreven in de voorgaande hoofdstukken. Het geleverde dient additioneel aan de hieronder staande eisen te voldoen:

Nadere invulling IBPD-4.1, 4.2 en 4.3

Eis	Omschrijving
IBPx-6.1	Privacy by default; contactinformatie wordt pas opgevraagd en doorgegeven van een klant bij actief aanvinken dat klant naar aanleiding van onderzoek wil worden gebeld.
IBPx-6.2	Bij open invulvelden is het mogelijk om waarschuwingsmeldingen te plaatsen. De invuller wordt gewaarschuwd om geen persoonlijke gegevens te delen zonder dat geënquêteerden dit weerhoudt van antwoorden en/of een impact heeft op lengte van de vragenlijst.

IBPx-6.3	
IBPx-6.4	De Opdrachtnemer dient te waarborgen dat er geen gevoelige informatie, waaronder maar niet beperkt tot BSN's, wordt vastgelegd of verwerkt in logbestanden.
IBPx-6.5	De Opdrachtnemer dient te waarborgen dat er geen verrijking van datasets plaatsvindt zonder voorafgaand overleg en uitdrukkelijke schriftelijke toestemming van de SVB.
IBPx-6.6	Er wordt gebruik gemaakt van software bij het versturen van uitnodigingen waarbij technisch en/of organisatorisch is afgedwongen dat respondenten geen inzage krijgen in elkaars contactgegevens (bijvoorbeeld door CC e-mail).
IBPx-6.7	Informatie van klanten uit onderzoek moet kunnen worden gekoppeld aan SVB-medewerkers door middel van gecodeerde unieke identifiers.

Nadere invulling IBPB-4.12

Eis	Omschrijving
	.

Nadere invulling IBPB-4.4, 4.5 en 4.15

Eis	Omschrijving
IBPx-6.11	Bij uitnodigingen wordt altijd vermeld dat deelnemen op vrijwillige basis, deelnemen niet verplicht is (opt-in) en dat wel of niet deelnemen geen gevolgen heeft. Daarbij kan actief worden geïnformeerd dat betrokkenen geen negatieve gevolgen voor hun recht op uitkering zullen ondervinden bij deelname.
IBPx-6.12	Indien klanten niet in aanmerking willen komen voor onderzoek, is er de mogelijkheid deze klanten bij voorbaat uit te sluiten.
IBPx-6.13	Klanten kunnen bij de uitnodiging, gedurende het onderzoek of daarna alsnog kenbaar maken niet te willen meewerken. Er is de mogelijkheid deze klanten uit te sluiten van verder onderzoek en resultaten.