

| Onderwerp | Omschrijving | Eis/wens | Voldoet | Onderbouwing/motivering |
|---|---|------------------------------|---------|-------------------------|
| Certificering | De Leverancier (verder te noemen; de Leverancier) is ISO27001 gecertificeerd. Dit dient aangetoond te worden middels een geldig en actueel certificaat. Indien de leverancier een dergelijke certificering niet bezit, toont de leverancier aan op welke wijze de beveiliging van persoonsgegevens dan is vormgegeven. | Eis | ja/nee | Eventuele onderbouwing |
| | De eigenaar van het datacenter waar de Leverancier servers c.q. clouddiensten heeft ondergebracht is ISO27001 gecertificeerd. | Indien van toepassing -> Eis | ja/nee | Eventuele onderbouwing |
| | De verwerker/eigenaar van het datacenter waar de leverancier eventuele server c.q. clouddiensten heeft ondergebracht beschikt over een actuele en geldige Assurance verklaring zoals een ISAE 3000 (SOC2) of soortgelijke verklaring met daarin als toetsingscriteria de Trust Services Principles (Security, Availability, Processing Integrity, Confidentiality en Privacy op basis van de Europese wetgeving) waaruit blijkt welke op het risico afgestemde technische en organisatorische maatregelen de verwerker of eigenaar van het datacenter waar de server c.q. cloudoplossing is ondergebracht heeft genomen, daadwerkelijk worden uitgevoerd en in stand worden gehouden. | Indien van toepassing -> Eis | ja/nee | Eventuele onderbouwing |
| Chief Information Security Officer (CISO) | De Leverancier heeft een Chief Information Security Officer (CISO) / security officer aangesteld of kent een vergelijkbare functionaris. | Wens | ja/nee | Eventuele onderbouwing |
| | De eigenaar van het datacenter waar de leverancier server c.q. clouddiensten heeft ondergebracht heeft een Chief Information Security Officer (CISO) / security officer aangesteld of vergelijkbaar. | Indien van toepassing -> Eis | ja/nee | Eventuele onderbouwing |
| Informatiebeveiligingsbeleid | De Leverancier beschikt over een up to date, actueel en door bevoegde orgaan vastgesteld informatiebeveiligingsbeleid. | Eis | ja/nee | Eventuele onderbouwing |
| | De verwerker/eigenaar van het datacenter waar de leverancier server c.q. clouddiensten heeft ondergebracht beschikt over een up to date, actueel en door de directie vastgesteld informatiebeveiligingsbeleid. | Indien van toepassing -> Eis | ja/nee | Eventuele onderbouwing |
| Dataclassificatie | De Leverancier heeft een dataclassificatie uitgevoerd op de categorieën van persoonsgegevens en de datavelden die door de Leverancier en/of bijbehorende applicatie(s) worden verwerkt. | Wens | ja/nee | Eventuele onderbouwing |
| PIA | De Leverancier heeft op basis van een privacy impact analyse (gegevensbeschermingseffectbeoordeling) de belangrijkste privacy risico's (binnen de Leverancier en bijbehorende applicatie(s)) in beeld gebracht. | Wens | ja/nee | Eventuele onderbouwing |
| Risicoanalyse | De Leverancier beschikt over een up to date / actuele risicoanalyse betreffende de Leverancier en bijbehorende applicatie(s). | Eis | ja/nee | Eventuele onderbouwing |
| Rechtmatigheid van de verwerking (art 6 AVG) Zie ook art 15 lid 1 sub a AVG -> Inzage in de verwerkingsdoeleinden. | De Leverancier en/of bijbehorende applicatie(s) kan vastleggen wat de "grondslag" is voor de werking. | Wens | ja/nee | Eventuele onderbouwing |
| Bijzondere categorieën van persoonsgegevens (art 9 Avg) | De Leverancier en/of bijbehorende applicatie(s) kan de verwerking van bijzondere persoonsgegevens identificeren. | Wens | ja/nee | Eventuele onderbouwing |
| Recht op inzage (art 15 AVG) | De Leverancier en/of bijbehorende applicatie(s) maakt de betrokken categorieën van persoonsgegevens/gebruikers zichtbaar. | Eis | ja/nee | Eventuele onderbouwing |
| | De Leverancier en/of bijbehorende applicatie(s) maakt de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt zichtbaar. | Eis | ja/nee | Eventuele onderbouwing |
| | De Leverancier en/of bijbehorende applicatie(s) biedt de mogelijkheid om aan de betrokkene(n) een kopie van de verwerkte persoonsgegevens in een gangbare elektronische vorm te verstrekken. | Eis | ja/nee | Eventuele onderbouwing |
| | Binnen de Leverancier en/of bijbehorende applicatie(s) is de mogelijkheid aanwezig om te loggen door wie en wanneer de persoonsgegevens zijn/werden verwerkt, ingezien of gemuteerd. | Wens | ja/nee | Eventuele onderbouwing |
| Recht op rectificatie (art 16 AVG) | Binnen de Leverancier en/of bijbehorende applicatie(s) kan een verbetering van onjuiste persoonsgegevens worden doorgevoerd. | Eis | ja/nee | Eventuele onderbouwing |
| | Deze correcties worden binnen de Leverancier en/of bijbehorende applicatie(s) gelogd. | Wens | ja/nee | Eventuele onderbouwing |
| Recht om te worden vergeten (art 17 AVG) | De Leverancier en/of bijbehorende applicatie(s) voorzien in de mogelijkheid op het recht om te worden vergeten. Oftewel gegevens kunnen definitief worden verwijderd, inclusief de koppeling naar, een kopie of reproductie. | Eis | ja/nee | Eventuele onderbouwing |

| | | | | |
|--|--|------|--------|------------------------|
| Geautomatiseerde individuele besluitvorming (art 22 AVG) | De door de leverancier gebruikte applicatie biedt geen mogelijkheid tot geautomatiseerde besluitvorming. | Eis | ja/nee | Eventuele onderbouwing |
| Privacy bij design en default (art 25 AVG) | De Leverancier en/of bijbehorende applicatie(s), zoals e-mail en administratieve applicaties voldoen aan de eis van Privacy bij design en default. Voor wat betreft het gebruik van e-mail applicaties/systemen voldoen deze ten minste aan de vereisten voor veilig gebruik, zoals bedoeld in NTA7516. | Eis | ja/nee | Eventuele onderbouwing |
| | De Leverancier en/of bijbehorende applicatie(s) voorzien in waarborging van de eis dat in beginsel alleen persoonsgegevens kunnen worden verwerkt die noodzakelijk zijn voor het specifieke doel van de verwerking. | Wens | ja/nee | Eventuele onderbouwing |
| De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling (artikel 28 AVG) | De leverancier sluit een (verwerkers)overeenkomst overeenkomstig het bepaalde de in artikel 28 AVG af met de gemeente. De gemeente maakt hiervoor gebruik van een voor de gemeente verplicht model van de VNG. | Eis | ja/nee | Eventuele onderbouwing |
| Verwerkingsregister | De leverancier beschikt over een verwerkingsregister dat voldoet aan de vereisten van artikel 30, lid 2 AVG | Eis | ja/nee | Eventuele onderbouwing |
| Beveiliging van de verwerking | De verwerker biedt afdoende garanties met betrekking tot de vertrouwelijkheid, integriteit, beschikbaarheid van de gegevens binnen de Leverancier en/of bijbehorende applicatie(s). | Eis | ja/nee | Eventuele onderbouwing |
| | De leverancier biedt afdoende garanties om de verwerkingsrisico's binnen de Leverancier en/of bijbehorende applicatie(s) als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig te minimaliseren. | Eis | ja/nee | Eventuele onderbouwing |
| Meldplicht datalekken (art 33 en 34 AVG) | De leverancier/verwerker verplicht zich om binnen uiterlijk 24 uur, alle (vermoedelijke) datalekken in verband met persoonsgegevens in zijn bedrijf en/of bij de personen onder zijn gezag (in loondienst of ingehuurd of anderszins tewerkgesteld) en/of bij zijn sub-verwerkers (met inbegrip van het datacenter, server en/of cloud) -die op grond van wetgeving moeten worden gemeld aan de toezichthouder of betrokkene te melden aan de Chief Information Security Officer (CISO) van de verwerkingsverantwoordelijke. | Eis | ja/nee | Eventuele onderbouwing |
| | Naast de meldplicht zoals hierboven geldt onverminderd de verplichting voor de verwerker om de gevolgen van dergelijke datalekken zo snel mogelijk ongedaan te maken dan wel te beperken | Eis | ja/nee | Eventuele onderbouwing |

OPM: Deze bijlage dient te worden ingevuld en aangeleverd als bewijsstuk, op het moment dat de Opdrachtgever dit vraagt, na aanmelding.