Belastingsamenwerking Oost-Brabant

Programma van Eisen - Informatiebeveiliging

Belastingsamenwerking Oost-Brabant

Datum	25-02-2026
Versie	1.0
Classificatie	Openbaar
Auteurs	Fouad Taheri, Hedwy van de Werf

Belastingsamenwerking Oost-Brabant

Inhoudsopgave

1. Toepasselijkheid en risicogebaseerde toepassing

Deze bijlage is van toepassing op iedere opdracht waarbij Opdrachtnemer toegang heeft tot, of gegevens verwerkt van, Opdrachtgever (BSOB), waaronder maar niet beperkt tot applicaties, systemen, cloudoplossingen en dienstverlening.

Indien sprake is van:

- verwerking van persoonsgegevens;
- verwerking van vertrouwelijke of financiële gegevens;
- structurele toegang tot systemen van Opdrachtgever;
- hosting of opslag van gegevens;
- ondersteuning van kritieke processen;
- zijn tevens de aanvullende eisen uit deze bijlage van toepassing.

2. Assurance & Compliance

2.1 Informatiebeveiligingscertificering

Eis: Opdrachtnemer toont aantoonbare beheersing van informatiebeveiliging aan door middel van:

- een geldig **ISO/IEC 27001-certificaat**,
  en/of
- een **ISAE 3000** of **3402 Type II** of **SOC 1 of SOC 2 Type II** assurance-rapport.

Het certificaat of rapport:

- is afgegeven door een onafhankelijke, geaccrediteerde partij;
- heeft betrekking op de aangeboden dienstverlening;
- is geldig gedurende de looptijd van de overeenkomst.

Op verzoek verstrekt Opdrachtnemer de volledige assurance-rapportage, inclusief management letter.

2.2 Minimale scope-eisen Certificaat/Assurance

Eis: Indien ISO 27001 en/of ISAE/SOC wordt gebruikt, dient de scope **minimaal** betrekking te hebben op:

- de software en dienstverlening geleverd aan opdrachtgever *(indien een softwarepakket wordt aangeschaft);*
- de verwerking, opslag en overdracht van data;
- gebruikte IT-systemen, infrastructuur en ondersteunende processen;
- betrokken personeel en relevante onderaannemers.

In de scope van de beveiligingsmaatregelen moeten minimaal de volgende thema's zijn afgedekt:

- toegangsbeveiliging/IAM (Identity & Access Management);
- logging en monitoring;
- incident- en datalekmanagement;
- Back-ups & continuïteit;
- ontwerp-, ontwikkel- en wijzigingsprocessen(indien van toepassing):
  - Security by Design
  - Secure Software Lifecycle
  - Secure by Default
- Kwetsbaarheden- en patchmanagement;
- uitbesteding en subverwerkers.

3. Data, Privacy & Juridische Compliance

3.1 Dataresidentie

Eis: Indien gegevens worden opgeslagen of gehost:

- worden alle gegevens, inclusief back-ups en logbestanden, uitsluitend binnen de Europese Unie verwerkt en opgeslagen;
- vindt doorgifte buiten de EU uitsluitend plaats na voorafgaande schriftelijke toestemming van Opdrachtgever en met passende waarborgen.

Deze verplichting geldt tevens voor subverwerkers.

3.2 Privacy by Design

Eis: De software ondersteunt privacy by design, waaronder:

- gegevensminimalisatie;
- doelbinding;
- ondersteuning van rechten van betrokkenen
- passende technische en organisatorische beveiligingsmaatregelen.

3.3 Verwerkersrol

Eis: Indien Opdrachtnemer persoonsgegevens verwerkt:

- treedt Opdrachtnemer op als verwerker conform artikel 28 AVG;
- wordt een verwerkersovereenkomst gesloten;
- blijven verplichtingen onverkort gelden voor subverwerkers;
- blijft Opdrachtnemer volledig verantwoordelijk voor naleving door subverwerkers.

Subverwerkers worden vooraf schriftelijk gemeld aan Opdrachtgever.

3.4 Data Protection Impact Assessment (DPIA)

Indien van toepassing verstrekt Opdrachtnemer relevante informatie ter ondersteuning van een Data Protection Impact Assessment (DPIA), waaronder:

- geïdentificeerde privacyrisico's;
- mitigerende maatregelen op applicatieniveau;
- resterende restrisico's.

4. Technische en Organisatorische Beveiliging

4.1 Encryptie

Eis: Opdrachtnemer past passende encryptiemaatregelen toe, waaronder:

- versleuteling van data in transit (minimaal TLS 1.2 of hoger);
- versleuteling van data at rest bij opslag (minimaal AES-256);
- adequaat sleutelbeheer.

4.2 Toegangsbeheer

Eis: Opdrachtnemer:

- past het least privilege-principe toe;
- hanteert multi-factor authenticatie voor beheerders;
- logt beheeractiviteiten;
- voert periodieke review uit op privileged accounts.

4.3 Logging en monitoring

Eis: Opdrachtnemer:

- registreert relevante beveiligingsgebeurtenissen;
- bewaart loggegevens gedurende een passende termijn (minimaal 6 maanden, tenzij anders overeengekomen);
- stelt relevante loggegevens op verzoek beschikbaar voor onderzoek
- meldt locatie(s) van datacenters.

4.4 Kwetsbaarheden en Patchmanagement

Eis: Opdrachtnemer:

- beschikt over een formeel patchmanagementproces;
- voert periodiek beveiligingstesten uit (waaronder penetratietesten indien van toepassing);
- beschikt over een responsible disclosure beleid;
- informeert Opdrachtgever onverwijld over kritieke kwetsbaarheden die impact hebben op de dienstverlening.

5. Incidentmanagement & Continuïteit

5.1 Melden van Incidenten

Eis: Opdrachtnemer beschikt over een formeel incidentmanagementproces.
Beveiligingsincidenten en datalekken worden:

- uiterlijk binnen 24 uur na ontdekking gemeld;
- binnen 72 uur voorzien van nadere impactanalyse en mitigerende maatregelen;
- volledig gedocumenteerd.

Ernstige incidenten dienen ***onverwijld*** te worden gemeld.

5.2 Continuïteit

Eis (voor SaaS applicaties): Opdrachtnemer beschikt over:

- een business continuity plan;
- vastgestelde hersteldoelstellingen (RTO/RPO);
- periodiek geteste herstelprocedures.

6. Service Level Agreement

Eis (voor SaaS applicaties): Opdrachtnemer rapporteert periodiek over:

- beschikbaarheid;
- incidenten en verstoringen;
- beveiligingsincidenten;
- relevante risico's en wijzigingen.

7. Contractuele voorwaarden

7.1 Beveiligingsverplichtingen en garanties

Eis: Opdrachtnemer blijft gedurende de looptijd van de overeenkomst voldoen aan de overeengekomen beveiligingseisen en certificeringen. Wijzigingen hierin worden onverwijld gemeld.

7.2 Aansprakelijkheid

Eis: Opdrachtnemer accepteert aansprakelijkheid voor schade als gevolg van:

- tekortkomingen in informatiebeveiliging;
- schending van privacywetgeving;
- structurele niet-naleving van service levels.

Beperkingen van aansprakelijkheid dienen redelijk en marktconform te zijn.

7.3 Auditrecht

Eis: Opdrachtgever heeft het recht om:

- assurance-rapportages in te zien;
- aanvullende toelichting te vragen;
- bij zwaarwegend belang een aanvullende audit uit te voeren of te laten uitvoeren.

7.4 Exitstrategie

Eis: Opdrachtnemer beschikt over een gedocumenteerde exitstrategie die waarborgt dat beëindiging van de dienstverlening gecontroleerd en zonder verlies van data of continuïteit plaatsvindt.

7.5 Dataportabiliteit & dataverwijdering

Eis: Bij beëindiging van de overeenkomst:

- kan opdrachtgever zijn data exporteren in een gangbaar, machineleesbaar formaat;
- wordt resterende data binnen een overeengekomen termijn aantoonbaar verwijderd.

7.6 Nazorg

Eis: Opdrachtnemer verleent redelijke medewerking aan een overgangsperiode naar een opvolgend leverancier.