

Bijlage 7 - Eisen aan de leverancier – EZK Cloudbeleid

1. De leverancier beschikt over een geldige ISO-27001 certificering en de volledige lifecycle van de cloud toepassing valt binnen de scope van deze certificering.
2. Er zijn afspraken aanwezig hoe overdracht van data en/of software geschiedt in geval van beëindiging van de overeenkomst en welke verplichtingen de leverancier hierin heeft (exit strategie).
3. De leverancier verplicht zich beveiligingsincidenten relevant aan de dienstverlening voor RVO binnen 4 uur na constatering rechtstreeks te melden aan het Security Office van RVO (rvoinformatiebeveiliging@rvo.nl) onder vermelding van de opdrachtgever binnen RVO.
4. De leverancier verplicht zich geconstateerde beveiligingsissues t.a.v. de door hen geleverde public cloud toepassing op te lossen. Hiertoe meldt de leverancier binnen 48 uur aan RVO de termijn waarop de oplossing gerealiseerd is.
5. De leverancier verplicht zich mee te werken aan audits op het gebied van informatiebeveiliging en privacy geïnitieerd door de opdrachtgever¹⁰.
6. De leverancier verplicht zich inzichtelijk te maken welke andere partijen betrokken zijn bij de invulling van de overeenkomst. Wijzigingen in de betrokken partijen worden schriftelijk gecommuniceerd aan de opdrachtgever binnen RVO én aan de RVO IMP Servicedesk.
7. Er zijn afspraken aanwezig op welke wijze de leverancier data binnen de contractuele doelbinding van de opdrachtgever doorgeeft aan derde partijen (bijv. backups, logfiles, telemetrie, etc.). Voor doorgifte van data binnen de contractuele doelbinding naar verwerkers buiten de EU/EER ruimte is expliciete toestemming nodig van de opdrachtgever.
8. Er zijn afspraken aanwezig op welke wijze de leverancier deelneemt aan de door RVO ingerichte crisis organisatie.

Als uit de expliciete risicoanalyse (Quickscan BIO) blijkt dat beschikbaarheid (B), integriteit (I) of vertrouwelijkheid (V) een score van midden of hoger oplevert dan gelden aanvullend de volgende extra eisen:

9. De leverancier kan aantonen dat voldaan wordt aan ISO-27017.
10. De leverancier past encryptie toe op de data. Encryptie wordt gebruikt voor data-in-rest, data-in-use en data-in-transit. Er zijn expliciete afspraken gemaakt met de leverancier over beheer van de encryptiesleutels.
11. Met de leverancier dient een SLA afgesloten te worden met een periodieke rapportage (frequentie afhankelijk van risicoprofiel). In de SLA rapportage dient tenminste aandacht te zijn gegeven aan onderstaande punten:
 - a) (ernstige) beveiligingsincidenten en de afhandeling daarvan
 - b) uitgevoerde beveiligingsscan (pentest, vulnerability scan, etc.)
 - c) veranderingen in derde partijen betrokken bij de dienstverlening