de Rechtspraak

IVO Rechtspraak

SaaS-leidraad <naam SaaS-dienst>

Datum	<datum>
Versie	<nr.>
Auteur(s)	<naam>, <naam>

Inhoud

Deel 1: Achtergrond en Restrisico's 3
1.1 Inleiding 3
1.2 Projectfasering (optioneel) 3
1.3 Doel van deze SaaS-leidraad 3
1.4 Te accepteren restrisico's 3

Deel 2: Onderbouwing van de Restrisico's 4
2.1 Toelichting op de gebruikte evidence om de Restrisico's te onderbouwen 4
2.2 Relevante externe ontwikkelingen en de beoordeling van het project (optioneel) 4
2.3 Toetsing aan het afwegingskader van het Rechtspraak Cloudbeleid 4
2.4 Toetsing aan de inrichtingsprincipes van het Rechtspraak Cloudbeleid 5
2.5 Toetsing aan de businessrisico's zoals geformuleerd in het Rechtspraak Cloudbeleid 6

Deel 1: Achtergrond en Restrisico's

1.1 Inleiding

<Geef kort aan om welke SaaS-dienst het gaat, wie de leverancier is, wat de kenmerken zijn en welke waarde deze voor de business heeft. Houd het kort, verwijs voor meer info naar de Lean Businesscase>

1.2 Projectfasering (optioneel)

<Onboarding van grote diensten – 5.1(2)h, 5.1(2)i – gebeurt vaak gefaseerd. Is dit het geval, beschrijf dan de fasering en op welke fase deze SaaS-leidraad betrekking heeft. Is dit niet het geval, haal deze paragraaf dan weg>

1.3 Doel van deze SaaS-leidraad

<voorbeeld tekst: Het doel van deze SaaS-leidraad is om de restrisico's in kaart te brengen die geaccepteerd moeten worden voordat de SaaS-dienst in gebruik kan worden genomen. De restrisico's zijn de risico's die overblijven nadat alle risicomitigerende maatregelen zijn genomen. Over het accepteren van de restrisico's beslissen in ieder geval de Portefeuillehouder en de Cloudregiegroep. De Cloudregiegroep bepaalt of de risico's ook ter besluitvorming aan Directie IVO worden voorgelegd. Directie IVO kan besluiten de restrisico's ook aan andere (business)overleggen voor te leggen, alvorens een beslissing te nemen (zie besluitvormingsproces in het Rechtspraak Cloudbeleid)>

1.4 Te accepteren restrisico's

<Som hier de restrisico's op die geaccepteerd moeten worden voordat de SaaS-dienst in gebruik kan worden genomen. Geef per restrisico een korte toelichting en maak waar relevant verwijzingen naar deel 2 van deze leidraad. Formuleer de restrisico's zorgvuldig! Geef zo concreet mogelijk aan wie welk risico loopt. Schets in de toelichting wat de kans van optreden is en wat de gevolgen daarvan zijn.>

Deel 2: Onderbouwing van de Restrisico's

2.1 Toelichting op de gebruikte evidence om de Restrisico's te onderbouwen

<Door het proces voor onboarding en monitoring van SaaS-diensten te volgen wordt 'evidence' verzameld. De evidence kan bijvoorbeeld bestaan uit de Lean Businesscase, BIA, Architectuurstatement, DPIA, Risicoanalyses, Contract, Verwerkingsovereenkomsten etc. Neem hier een overzicht op van de evidence die relevant is voor het onderbouwen van de restrisico's>

2.2 Relevante externe ontwikkelingen en de beoordeling van het project (optioneel)

<Soms kunnen externe ontwikkelingen relevant zijn voor het beoordelen van restrisico's. Bijvoorbeeld afwegingen en besluiten van andere organisaties op dezelfde risico's, of politiek/bestuurlijke discussies. Als er geen relevante externe ontwikkelingen zijn, haal deze paragraaf dan weg>

2.3 Toetsing aan het afwegingskader van het Rechtspraak Cloudbeleid

Het Rechtspraak Cloudbeleid beschrijft de randvoorwaarden, oftewel de spelregels, voor het toepassen van externe clouddiensten. Vanuit deze Rechtspraak Cloudbeleid wordt gevraagd invulling te geven op het cloud afwegingskader door het beantwoorden van 5 kernvragen.

Kernvraag 1

Zijn de beschikbaarheid, integriteit en vertrouwelijkheid van de data en de geleverde IV-dienst alsmede privacy voldoende gewaarborgd en wordt daarbij voldaan aan wet en regelgeving?

<Geef antwoord op de vraag, onderbouw dit met de verzamelde evidence (zie 2.1) en geef aan wat eventuele restrisico's zijn>

Kernvraag 2

Is er voldoende vertrouwen in de leverancier(s) en in het vermogen van de Rechtspraak (IVO) om deze aan te sturen?

<Geef antwoord op de vraag, onderbouw dit met de verzamelde evidence (zie 2.1) en geef aan wat eventuele restrisico's zijn>

Kernvraag 3

Zijn risico's die de leverancier vormt voor de staatsrechtelijke onafhankelijkheid in beeld en voldoende gemitigeerd?

<Geef antwoord op de vraag, onderbouw dit met de verzamelde evidence (zie 2.1) en geef aan wat eventuele restrisico's zijn>

Kernvraag 4

Is de weerbaarheid tegen zgn. 'advanced persistent threats' op voldoende niveau?

<Geef antwoord op de vraag, onderbouw dit met de verzamelde evidence (zie 2.1) en geef aan wat eventuele restrisico's zijn>

Kernvraag 5
Is er een realistische exit-strategie?
<Geef antwoord op de vraag, onderbouw dit met de verzamelde evidence (zie 2.1) en geef aan wat eventuele restrisico's zijn>

2.4 Toetsing aan de inrichtingsprincipes van het Rechtspraak Cloudbeleid

Principe 1
Als staatsgeheim geclassificeerde data en stukken worden niet in een externe cloud verwerkt.
<Geef aan of aan het principe wordt voldaan, wat eventueel afwijkingen zijn en of dat tot een restrisico leidt. Maak gebruik van de verzamelde evicence>

Principe 2
De voorzitter van een zeer gevoelige rechtszaak kan samen met het gerechtsbestuur besluiten om bij de zaak horende data en stukken niet in een externe cloud te verwerken.
<Geef aan of aan het principe wordt voldaan, wat eventueel afwijkingen zijn en of dat tot een restrisico leidt. Maak gebruik van de verzamelde evicence>

Principe 3
Hoog of zeer hoog vertrouwelijk geclassificeerde data en stukken, alsmede bijzondere persoonsgegevens en medische gegevens worden alleen in een externe cloud verwerkt nadat: 1. een onafhankelijke check op de beveiligingsmaatregelen van de betreffende clouddienst heeft plaatsgevonden en 2. de S&I Board met het gebruik van de clouddienst heeft ingestemd.
<Geef aan of aan het principe wordt voldaan, wat eventueel afwijkingen zijn en of dat tot een restrisico leidt. Maak gebruik van de verzamelde evicence>

Principe 4
Vertrouwelijk of hoger geclassificeerde data en stukken, alsmede persoonsgegevens worden binnen de EU/EER verwerkt.

Principe 5
Vertrouwelijk of hoger geclassificeerde data en stukken, alsmede persoonsgegevens zijn gedurende opslag en transport versleuteld. De Rechtspraak richt het sleutelbeheer zelf in.
<Geef aan of aan het principe wordt voldaan, wat eventueel afwijkingen zijn en of dat tot een restrisico leidt. Maak gebruik van de verzamelde evicence>

Principe 6
Identity en access management houdt de Rechtspraak in eigen hand.
<Geef aan of aan het principe wordt voldaan, wat eventueel afwijkingen zijn en of dat tot een restrisico leidt. Maak gebruik van de verzamelde evicence>

Principe 7
Het voornemen om een clouddienst van een ketenpartner af te nemen wordt ter instemming voorgelegd aan de S&I Board.
<Geef aan of aan het principe wordt voldaan, wat eventueel afwijkingen zijn en of dat tot een restrisico leidt. Maak gebruik van de verzamelde evicence>

2.5 Toetsing aan de businessrisico's zoals geformuleerd in het Rechtspraak Cloudbeleid

Risico 1
Geen gecontroleerde scheiding tussen de procesdata/-stukken van de Rechtspraak en die van andere procespartijen
<Geef aan of hiervoor gevonden restrisico's betrekking hebben op dit businessrisico en hoe het restrisico zich voor de business manifesteert. Zie evt. de beschrijving van dit businessrisico in het Cloudbeleid>

Risico 2
Niet in control op beveiliging van en autorisatie voor Rechtspraak data, stukken en/of verkeersgegevens
<Geef aan of hiervoor gevonden restrisico's betrekking hebben op dit businessrisico en hoe het restrisico zich voor de business manifesteert. Zie evt. de beschrijving van dit businessrisico in het Cloudbeleid>

Risico 3
Door continuïteitsproblemen in de IV ook continuïteitsproblemen in de Rechtspraak dienstverlening
<Geef aan of hiervoor gevonden restrisico's betrekking hebben op dit businessrisico en hoe het restrisico zich voor de business manifesteert. Zie evt. de beschrijving van dit businessrisico in het Cloudbeleid>

Risico 4
De Rechtspraak maakt zich te afhankelijk van de 'big-tech' bedrijven
<Geef aan of hiervoor gevonden restrisico's betrekking hebben op dit businessrisico en hoe het restrisico zich voor de business manifesteert. Zie evt. de beschrijving van dit businessrisico in het Cloudbeleid>

Risico 5
Data/stukken worden gevorderd door statelijke actoren op grond van hun eigen wetgeving
<Geef aan of hiervoor gevonden restrisico's betrekking hebben op dit businessrisico en hoe het restrisico zich voor de business manifesteert. Zie evt. de beschrijving van dit businessrisico in het Cloudbeleid>

Risico 6

Statelijke actoren stelen zeer vertrouwelijke data/stukken of plegen digitale sabotage

<Geef aan of hiervoor gevonden restrisico's betrekking hebben op dit businessrisico en hoe het restrisico zich voor de business manifesteert. Zie evt. de beschrijving van dit businessrisico in het Cloudbeleid>

Risico 7

Door hacks krijgt de georganiseerde misdaad toegang tot systemen en/of zaaksgebonden data/stukken

<Geef aan of hiervoor gevonden restrisico's betrekking hebben op dit businessrisico en hoe het restrisico zich voor de business manifesteert. Zie evt. de beschrijving van dit businessrisico in het Cloudbeleid>

Risico 8

De Rechtspraak is te afhankelijk van IV-diensten van ketenpartners

<Geef aan of hiervoor gevonden restrisico's betrekking hebben op dit businessrisico en hoe het restrisico zich voor de business manifesteert. Zie evt. de beschrijving van dit businessrisico in het Cloudbeleid>