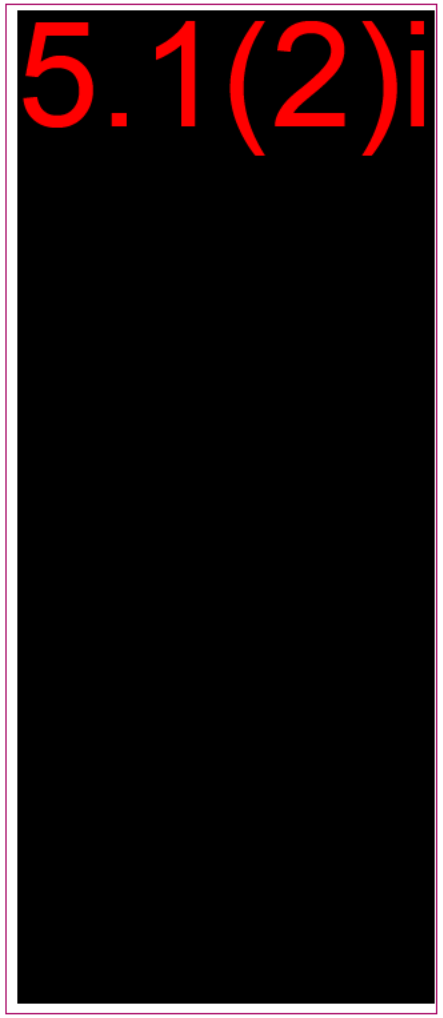
CONCEPT

Handreiking SaaS-diensten en persoonsgegevens gebruikers

Hoe om te gaan met persoonsgegevens van gebruikers die nodig zijn voor de technische werking van SaaS-diensten?

Versie: 0.8
Auteurs: 5.1(2)e

Probleemanalyse



Complicatie

- Doordat er geen afgesproken mate van risicobereidheid is en de risico's en maatregelen per SaaS-dienst afzonderlijk worden beoordeeld:
  - is het beoordelingsproces arbeidsintensief;
  - is de doorlooptijd van het proces lang;
  - is de voorspelbaarheid van de uitkomst van een beoordeling laag;
  - kunnen er inconsistent besluiten genomen worden m.b.t. de acceptatie van risico's, die moeilijk uit te leggen zijn.

Vraag

- Hoe kunnen we de beoordeling van risico's en maatregelen, die samenhangen met het verlenen van toegang tot persoonsgegevens t.b.v. de technische werking van SaaS-diensten gemakkelijker, sneller, voorspelbaarder en consistenter maken?

Antwoord

- Door een afwegingskader dat toegepast kan worden in veelvoorkomende situaties.

Inleiding

In de Cloudstrategie en Technologiestrategie staat dat IVO voor standaardapplicaties vaker gebruik wil maken van SaaS-diensten. Het betreft applicaties waar geen maatwerk voor nodig is en die vooral in het domein Bedrijfsvoering (incl. werkplek) worden toegepast. Het gebruik van SaaS-diensten biedt flexibiliteit. Daarnaast ontzorgt het de afnemer, mits de risico's voldoende beheerst worden.

SaaS-diensten bieden de gebruiker functionaliteit voor het verwerken van informatie. Welke functionaliteit en informatie verwerkt wordt, verschilt uiteraard per SaaS-dienst. De risico's die samenhangen met het gebruik van SaaS-diensten en de beheersmaatregelen die nodig zijn, hangen o.a. af van de informatie die verwerkt wordt. Het 'onboarden' (het proces van selectie, inkoop en ingebruikname) van SaaS-diensten verloopt via een vast proces, dat aansluit op het Rechtspraak Cloudbeleid. Bijzondere aandacht gaat daarbij uit naar het beoordelen en mitigeren van risico's op het gebied van security en privacy. De Cloudregiegroep toetst per SaaS-dienst of het proces voor 'onboarden' goed doorlopen wordt.

Deze handreiking heeft betrekking op de verwerking van persoonsgegevens en daarmee privacy (andere aspecten, zoals security, worden apart beoordeeld). Om te beoordelen of persoonsgegevens verwerkt mogen worden en, zo ja, onder welke voorwaarden, wordt een Data Protection Impact Assessment (DPIA) uitgevoerd. Het beleid binnen de Rechtspraak (zie Minimumnorm Privacy) is dat voor elke nieuwe of veranderende verwerking van persoonsgegevens een DPIA moet worden gedaan. Dit is om de verwerking van de persoonsgegevens te kunnen toetsen aan privacy wetgeving, de risico's in beeld te brengen en de mitigerende maatregelen te bepalen.

Het gaat in deze handreiking echter niet om alle persoonsgegevens, maar om een specifieke categorie. Het gaat alleen om de persoonsgegevens die noodzakelijk zijn voor de technische werking van de SaaS dienst. Dit zijn de gegevens die gebruikt worden om een veilige verbinding te leggen tussen de Rechtspraak en de leverancier en die nodig zijn om de gebruiker toegang te geven tot de applicatie en zichzelf te kunnen identificeren als bevoegd gebruiker. Deze handreiking ziet niet op de overige persoonsgegevens die gebruikers verwerken middels de door de SaaS-dienst aangeboden functionaliteit.

Een DPIA is noodzakelijk voor de verwerking van beide categorieën van gegevens. Deze handreiking is bedoeld om voorafgaand aan de DPIA al handvatten mee te geven voor het bepalen van mogelijke risico's en mitigerende maatregelen m.b.t. persoonsgegevens die noodzakelijk zijn voor de technische werking van de SaaS-dienst. Zo kunnen al in een voorstadium stappen gezet worden om risico's te bepalen en wegen, mitigerende maatregelen te nemen en keuzes m.b.t. mogelijke oplossingsscenario's te maken.

Scope van deze handreiking

Deze handreiking heeft betrekking op:

Het beoordelen van de risico's en maatregelen…

bij het verlenen van toegang tot persoonsgegevens aan leveranciers (verwerkers) en onderleveranciers (subverwerkers) van SaaS-diensten…

voor zover het gegevens over de gebruiker betreft, die nodig zijn voor een correcte technische werking van de dienst.

Deze handreiking heeft geen betrekking op:

Andere diensten dan SaaS-diensten.

Persoonsgegevens die gebruikers van de SaaS-dienst verwerken middels de aangeboden functionaliteit.

Standaard verwerking persoonsgegevens

Ten behoeve van een correcte technische werking van SaaS-diensten worden vaak de volgende persoonsgegevens van de gebruiker verwerkt:

- E-mailadres
- Voornaam (afleidbaar uit gebruikersnaam of e-mailadres)
- Achternaam (afleidbaar uit e-mailadres)
- Initialen (afleidbaar uit e-mailadres)
- Gebruikersnaam
- Wachtwoord (indien geen SSO via Rechtspraak IAM)
- IP-adres (door VPN toegekend)

Richtlijn bij veel voorkomende situaties (1 van 6)

Hieronder genoemde veel voorkomende situaties zijn gebaseerd op een combinatie van de volgende factoren:

1. Persoonsgegevens (zie slide 5) worden alleen binnen de Europese Economische Ruimte (EER) verwerkt vs. persoonsgegevens worden (ook) buiten de EER verwerkt
   a. Bij verwerking buiten de EER: dit gebeurt structureel vs. dit gebeurt alleen in specifieke gevallen (onder bijzondere omstandigheden)
   b. Bij verwerking buiten de EER: dit gebeurt alleen in een land/landen waarvoor 1. een adequaatheidsbesluit geldt, 2. de leverancier goedgekeurde Binding Corporate Rules heeft of 3. de leverancier meedoet aan het Data Privacy Framework (geldt alleen voor de VS) vs. het betreft (ook) een land/landen zonder dat deze waarborgen van toepassing zijn
2. Het betreft persoonsgegevens van ondersteunende medewerkers vs. het betreft ook persoonsgegevens van mensen met een gevoelige functie, zoals rechters

NB. Deze handreiking schetst een aantal scenario's waarbij persoonsgegevens die noodzakelijk zijn voor de technische werking van de SaaS dienst (mogelijk) buiten de EER worden verwerkt. Dit wijkt af van het vigerende Cloudbeleid, waarin staat dat persoonsgegevens binnen de EER verwerkt moeten worden (zie inrichtingsprincipe 4). Momenteel wordt geschreven aan een nieuwe versie van het Cloudbeleid, waarin meer nuance in dit principe wordt aangebracht. Zolang het huidige Cloudbeleid van kracht is moet een afwijking op inrichtingsprincipe 4 vermeld en onderbouwd worden in de SaaS-leidraad (zie slides 7 t/m 10).

Richtlijn bij veel voorkomende situaties (2 van 6)

Situatie A. Persoonsgegevens blijven aantoonbaar binnen de EER

Onderstaande aanpak en maatregelen kunnen de risico's vaak tot een acceptabel niveau beperken

1. Alle leveranciers, dus ook onderleveranciers (subverwerkers) die worden ingezet (incl. moeder- of dochtermaatschappijen van de leverancier), zijn aantoonbaar binnen de EER gevestigd.
   NB. Indien dit niet het geval is, brengt dit extra risico's met zich mee en is situatie A niet van toepassing.
2. De leverancier (verwerker) verwerkt de persoonsgegevens, die noodzakelijk zijn voor de technische werking, aantoonbaar niet voor andere of eigen doeleinden zoals monitoring, nieuwsbrieven etc.
3. Bij de risicoafweging die het Cloudbeleid voorschrijft, is rekening gehouden met de reputatie van de leverancier en van diens onderleveranciers (zie kernvraag 2 van het afwegingskader in het Cloudbeleid).
4. De leverancier gaat akkoord met het afsluiten van de standaard verwerkersovereenkomst bij gunning (zonder afwijkingen te eisen).
5. De DPIA is op een van de volgende wijzen uitgevoerd en beoordeeld:
   a) Indien er sprake is van een 'off the shell' SaaS dienst waar we zelf geen aanpassingen aan doen, dan is de DPIA van de leverancier m.b.t. de technische werking van de applicatie opgevraagd en gezamenlijk met een privacy functionaris beoordeeld.
   b) Indien we wel aanpassingen aan de dienst doen, de leverancier geen DPIA heeft gedaan, deze niet wil verstrekken of de DPIA niet voldoet, dan is er een 'eigen' DPIA uitgevoerd (en voorzien van positief advies door de FG).

Richtlijn bij veel voorkomende situaties (3 van 6)

Situatie B. Persoonsgegevens worden alleen in specifieke gevallen (onder bijzondere omstandigheden) buiten de EER verwerkt

Onder een kleine kans verstaan we bijvoorbeeld:

- De leverancier kan niet uitsluiten dat gegevens bij een grootschalige verstoring van netwerken/systemen in de EER naar buiten de EER worden (om)geleid.
- In specifieke gevallen worden dienstverleners buiten de EER ingezet voor bijvoorbeeld het oplossen van incidentele helpdeskvragen of verstoringen (deze dienstverleners hebben dus niet continu toegang tot de persoonsgegevens). Let op: in geval van helpdeskvragen mag alleen het e-mailadres worden gedeeld (en dus de gegevens die daaruit zijn af te leiden, zoals voor- en achternaam). De overige gegevens mogen in dat geval niet worden gedeeld (dus ook niet de gegevens uit de handtekening van de medewerker)
- Met voorgaande punten vergelijkbare omstandigheden (bij twijfel, neem dan contact op met een privacy functionaris).

Indien sprake is van een kleine kans, dan kunnen de risico's met onderstaande aanpak en maatregelen vaak tot een acceptabel niveau beperkt worden

- De leverancier en evt. onderleveranciers (incl. moeder- of dochtermaatschappijen) zitten inderdaad binnen de EER en er is sprake van 'een kleine kans' dat persoonsgegevens buiten de EER worden verwerkt, zoals hierboven geschetst.
- De leverancier gaat akkoord gaat met het afsluiten van de standaard verwerkersovereenkomst bij gunning (zonder afwijkingen te eisen).
- De leverancier heeft onderbouwd in welke specifieke en slechts incidentele gevallen de persoonsgegevens buiten de EER zouden kunnen worden verwerkt en dit is vastgelegd (inclusief de noodzakelijke waarborgen die (moeten) worden getroffen) in de verwerkersovereenkomst. Een en ander is beoordeeld door de privacy functionaris.
- De leverancier (verwerker) verwerkt de persoonsgegevens, die noodzakelijk zijn voor de technische werking, aantoonbaar niet voor andere of eigen doeleinden zoals monitoring, nieuwsbrieven etc.
- Bij de risicoafweging die het Cloudbeleid voorschrijft is rekening gehouden met de reputatie van de leverancier en diens onderleveranciers (zie kernvraag 2 van het afwegingskader in het Cloudbeleid) alsmede met de reputatie van de landen waar zij zijn gevestigd, dan wel van de landen waar zij persoonsgegevens verwerken of zouden kunnen verwerken (al is het maar in theorie).
- Er is een DPIA uitgevoerd (en voorzien van positief advies door de FG).
- In de SaaS-leidraad is opgenomen welke restrisico's uit de DPIA naar voren komen, als gevolg van de mogelijke verwerking van persoonsgegevens buiten de EER. Indien van toepassing is onderbouwd waarom het acceptabel is om van inrichtingsprincipe 4 uit het Cloudbeleid af te wijken.

Is het aannemelijk dat specifieke gevallen met enige regelmaat voorkomen, zie C en D.

Richtlijn bij veel voorkomende situaties (4 van 6)

Situatie C. Persoonsgegevens worden buiten de EER verwerkt, maar alleen in een land/landen waarvoor een adequaatheidsbesluit geldt, de leverancier goedgekeurde Binding Corporate Rules heeft of de leverancier meedoet aan het Data Privacy Framework (geldt alleen voor de VS)

Indien het gegevens betreft van ondersteunende medewerkers, dan kunnen de risico's met onderstaande maatregelen vaak tot een acceptabel niveau beperkt worden (zie de volgende sheet indien het (ook) gegevens van mensen met een gevoelige functie betreft)

- Raadpleeg in dit geval altijd de privacy functionaris.
- Ga na (indien er geen adequaatheidsbesluit geldt) of de verwerking en/of het product/de dienstverlening van de leverancier onder de Binding Corporate Rules of het Data Privacy Framework valt.
- Toets of de leverancier akkoord gaat met het afsluiten van de standaard verwerkersovereenkomst bij gunning (zonder afwijkingen te eisen).
- Check in overleg met een privacy officer en security officer, welke privacy en security risico's volgen uit lokale wetgeving. Maak goede afspraken met de leverancier om de vastgestelde risico's te mitigeren en leg deze afspraken vast in de verwerkersovereenkomst.
- Vraag de leverancier om de bijlagen bij de standaard verwerkersovereenkomst en de Standard Contractual Clauses (SCC) in te vullen en leg deze vervolgens ter beoordeling voor aan een privacy functionaris en een security functionaris om de inhoud te toetsen.
- Check in welke landen de door de leverancier ingeschakelde onderleveranciers (en diens moeder- en dochtermaatschappijen) zijn gevestigd en waar de persoonsgegevens worden verwerkt. Voer voor de onderleveranciers die buiten de EER zijn gevestigd eenzelfde risicoafweging (inclusief het nemen van mitigerende maatregelen) uit.
- Toets of de leverancier de persoonsgegevens, die noodzakelijk zijn voor de technische werking, nog voor andere doeleinden gebruikt zoals monitoring, nieuwsbrieven etc. Indien dit het geval is, neem dan contact op met privacy functionaris.
- Houd bij de risicoafweging rekening met de reputatie van de leverancier en diens onderleveranciers (zie ook kernvraag 2 van het afwegingskader in het Cloudbeleid) alsmede met de reputatie van de landen waar zij zijn gevestigd, dan wel van de landen waar zij persoonsgegevens verwerken of zouden kunnen verwerken (al is het maar in theorie).
- Voer de DPIA uit.
- Neem in de SaaS-leidraad op welke restrisico's uit de DPIA naar voren komen, als gevolg van de mogelijke verwerking van persoonsgegevens buiten de EER. Onderbouw (indien van toepassing) waarom het acceptabel is om van inrichtingsprincipe 4 uit het Cloudbeleid af te wijken.

Richtlijn bij veel voorkomende situaties (5 van 6)

CONCEPT

Situatie D. Persoonsgegevens worden buiten de EER verwerkt, maar alleen in een land/landen waarvoor een adequaatheidsbesluit geldt, de leverancier goedgekeurde Binding Corporate Rules heeft of de leverancier meedoet aan het Data Privacy Framework (geldt alleen voor de VS)

Indien het (ook) gegevens van mensen met een gevoelige functie betreft, dan kunnen de risico's met onderstaande maatregelen vaak tot een acceptabel niveau beperkt worden

- Raadpleeg in dit geval altijd de privacy functionaris.
- Ga na (indien er geen adequaatheidsbesluit geldt) of de verwerking en/of het product/de dienstverlening van de leverancier onder de Binding Corporate Rules of het Data Privacy Framework valt.
- Toets of de leverancier akkoord gaat met het afsluiten van de standaard verwerkersovereenkomst bij gunning (zonder afwijkingen te eisen).
- Check, in overleg met een privacy officer en security officer, welke privacy en security risico's volgen uit lokale wetgeving. Maak goede afspraken met de leverancier om de vastgestelde risico's te mitigeren en leg deze afspraken vast in de verwerkersovereenkomst. Denk hierbij ook aan extra (beveiligings)maatregelen die kunnen worden genomen, waaronder maar niet beperkt tot encryptie of pseudonimisering, om de gegevens van mensen met een gevoelige functie die buiten de EER worden verwerkt zoveel mogelijk te beperken.
- Zorg dat de door de leverancier ingeschakelde onderleveranciers zo veel mogelijk worden beperkt tot de strikt noodzakelijke onderleveranciers.
- Vraag de leverancier om de bijlagen bij de standaard verwerkersovereenkomst en de SCC in te vullen en leg deze vervolgens ter beoordeling voor aan een privacy functionaris en een security functionaris om de inhoud te toetsen.
- Check in welke landen de door de leverancier ingeschakelde onderleveranciers (en diens moeder- en dochtermaatschappijen) zijn gevestigd en waar de persoonsgegevens worden verwerkt. Voer voor de onderleveranciers die buiten de EER zijn gevestigd eenzelfde risicoafweging (inclusief het nemen van mitigerende maatregelen) uit.
- Toets of de leverancier de persoonsgegevens, die noodzakelijk zijn voor de technische werking, nog voor andere doeleinden gebruikt zoals monitoring, nieuwsbrieven etc. Indien dit het geval is, neem dan contact op met privacy functionaris.
- Houd bij de risicoafweging rekening met de reputatie van de leverancier en diens onderleveranciers (zie ook kernvraag 2 van het afwegingskader in het Cloudbeleid) alsmede met de reputatie van de landen waar zij zijn gevestigd, dan wel van de landen waar zij persoonsgegevens verwerken of zouden kunnen verwerken (al is het maar in theorie).
- Voer de DPIA uit.
- Neem in de SaaS-leidraad op welke restrisico's uit de DPIA naar voren komen, als gevolg van de mogelijke verwerking van persoonsgegevens buiten de EER. Onderbouw (indien van toepassing) waarom het acceptabel is om van inrichtingsprincipe 4 uit het Cloudbeleid af te wijken.
- Voer binnen afzienbare tijd audits uit om te zien of zowel de leverancier als de door de leverancier ingeschakelde onderleveranciers de gemaakte afspraken nakomen.

Richtlijn bij veel voorkomende situaties (6 van 6)

Situatie E. Persoonsgegevens worden buiten de EER verwerkt, in een land/landen zonder een adequaatheidsbesluit, door een leverancier die geen goedgekeurde Binding Corporate Rules heeft of niet meedoet aan het Data Privacy Framework (voor de VS)

Minimaliseer de risico's met onderstaande maatregelen én maak een afweging tussen risico's en baten. Lukt het niet om onderstaande maatregelen te treffen, overweeg dan een alternatief dat valt onder A t/m C of kies voor een ander dienstverleningsmodel dan SaaS.

- Raadpleeg in dit geval altijd de privacy functionaris.
- Toets of de leverancier akkoord gaat met het afsluiten van de standaard verwerkersovereenkomst en de SCC bij gunning (zonder afwijkingen te eisen).
- Check, in overleg met een privacy officer en security officer, welke privacy en security risico's volgen uit lokale wetgeving. Maak goede afspraken met de leverancier om de vastgestelde risico's te mitigeren en leg deze afspraken vast in de verwerkersovereenkomst. Denk hierbij ook aan extra (beveiligings)maatregelen die kunnen worden genomen, waaronder maar niet beperkt tot encryptie of pseudonimisering, om de gegevens van mensen met een gevoelige functie die buiten de EER worden verwerkt zoveel mogelijk te beperken.
- Zorg dat de door de leverancier ingeschakelde onderleveranciers zo veel mogelijk worden beperkt tot de strikt noodzakelijke onderleveranciers.
- Vraag de leverancier om de bijlagen bij de standaard verwerkersovereenkomst en de SCC in te vullen en leg deze vervolgens ter beoordeling voor aan een privacy functionaris en een security functionaris om de inhoud te toetsen.
- Check in welke landen de door de leverancier ingeschakelde onderleveranciers (en diens moeder- en dochtermaatschappijen) zijn gevestigd en waar de persoonsgegevens worden verwerkt. Voer voor de onderleveranciers die buiten de EER zijn gevestigd eenzelfde risicoafweging (inclusief het nemen van mitigerende maatregelen) uit.
- Toets of de leverancier de persoonsgegevens, die noodzakelijk zijn voor de technische werking, nog voor andere doeleinden gebruikt zoals monitoring, nieuwsbrieven etc. Indien dit het geval is, neem dan contact op met privacy functionaris
- Houd bij de risicoafweging rekening met de reputatie van de leverancier en diens onderleveranciers (zie ook kernvraag 2 van het afwegingskader in het Cloudbeleid) alsmede met de reputatie van de landen waar zij zijn gevestigd, dan wel van de landen waar zij persoonsgegevens verwerken of zouden kunnen verwerken (al is het maar in theorie).
- Voer de DPIA uit.
- Neem in de SaaS-leidraad op welke restrisico's uit de DPIA naar voren komen, als gevolg van de mogelijke verwerking van persoonsgegevens buiten de EER. Onderbouw (indien van toepassing) waarom het acceptabel is om van inrichtingsprincipe 4 uit het Cloudbeleid af te wijken.
- Voer binnen afzienbare tijd audits uit om te zien of zowel de leverancier als de door de leverancier ingeschakelde onderleveranciers de gemaakte afspraken nakomen.