

Amerikaanse leveranciers in gebruik: wat zijn de effecten op de privacybescherming?

SURF Vendor Compliance voert DPIA's (gegevensbeschermingseffectbeoordelingen) uit. Hierbij wordt een analyse gemaakt van de privacyrisico's voor betrokkenen (gebruikers) op grond van de AVG. In veel gevallen zijn deze leveranciers Amerikaans of in handen van Amerikaanse eigenaren.

EU US Data Privacy Framework

Voor de doorgifte van persoonsgegevens naar Cloud/SaaS/PaaS leveranciers met een (hoofd)kantoor in de Verenigde Staten geldt momenteel dat er een adequaat beschermingsniveau voor persoonsgegevens is. Als leveranciers in de VS deelnemen aan het EU US Data Privacy Framework, kunnen zij de persoonsgegevens volgens het adequaatheidsbesluit van de Europese Commissie voldoende beschermen. Dat besluit geldt ook als Amerikaanse overheidsorganisaties en diensten toegang eisen tot gegevens die in Europa zijn opgeslagen. Omdat er momenteel sprake is van voldoende adequate bescherming zijn er geen aanvullende DTIA's (Data Transfer Impact Assessment) nodig.

Mogelijke risico's van geopolitieke ontwikkelingen

Gezien de geopolitieke ontwikkelingen in de VS is intrekking van het adequaatheidsbesluit niet ondenkbaar. Indien dit het geval is, kan er niet meer worden teruggevallen op het eerdergenoemde Data Privacy Framework. Als dat gebeurt, moeten we gebruik maken van andere juridische mechanismes voor doorgifte. Het is daarom goed hier al op voor te bereiden. Sluit daarom altijd Standard Contractual Clauses (SCCs) af. Naast SCCs dient dan ook een DTIA uitgevoerd te worden. Dit geldt ook voor verdere doorgifte naar andere landen dan de VS waarvoor niet de juiste waarborgen bestaan.

Bovendien moet waar mogelijk gebruik gemaakt worden van versleuteling van de persoonsgegevens, met een sleutel die exclusief in eigen beheer is. We kunnen dan niet vertrouwen op versleuteling door de leverancier.

Ook moeten we rekening houden met het risico dat (persoons)gegevens plotseling niet meer beschikbaar zijn als gevolg van Amerikaanse beleidsmaatregelen die de Amerikaanse leverancier kunnen dwingen om de diensten niet langer te leveren onder de overeengekomen juridische en financiële voorwaarden. Dit is met name van belang voor kritieke processen waarvoor het onaanvaardbaar is als deze diensten niet beschikbaar zijn.

SURF strategie

SURF stelt publieke waarden centraal binnen de diensten die we leveren en inkopen. We volgen hierbij de SURF-waardenwijzer die staat voor autonomie, menselijkheid en rechtvaardigheid. In de SURF Cloud Sourcing Strategie wordt verder toegelicht hoe we vanuit deze waarden zorgvuldig keuzes maken voor zaken die we inkopen.

Eén van de onderdelen in de SURF Cloud Sourcing Strategie gaat over het volgen van een multivendor strategie. Dat wil zeggen dat SURF met meerdere leveranciers overeenkomsten onderhandelt om afhankelijkheid van één enkele partij te voorkomen.

Bij het bepalen van de prioriteiten voor het sluiten van overeenkomsten en het uitvoeren van DPIA's ligt de focus in de praktijk nu op Europese leveranciers. Daarnaast blijft SURF continu met alle leveranciers in gesprek om te zorgen dat de sector veilig en verantwoord gebruik kan blijven maken van digitale onderwijsdiensten.