Criteria bij de keuze van applicaties voor de Leveranciers Compliance Dienstverlening

Openliggende privacy en securityvraagstukken, zoals:

- risico's van datadoorgifte naar derde landen, het (al dan niet hebben van SCC's) en de locatie van dataopslag;
- indicaties dat er voor de applicatie afspraken met de leverancier niet op orde zijn, zoals: verwerkersovereenkomsten, onduidelijkheden met de leverancier over de rollen van verantwoordelijke en verwerker;
- onduidelijkheden over welke data binnen de applicatie door de leverancier wordt verwerkt, hoeveel en hoe lang dit bewaard wordt,
- eerdere datalekken of serieuze security incidenten die hebben plaatsgevonden in de applicatie;
- het al dan niet op orde hebben van (security) certificeringen, zoals ISO 270001, ISO 27701 en ISAE 3402 type 2.

De ingediende wensen voor compliance trajecten worden gewogen op basis van:

- het aantal keer dat een leverancier wordt vermeld en de spreiding over de sectoren;
- het aantal instellingen en gebruikers van de applicatie;
- de hoeveelheid gebruikte persoonsgegevens binnen de applicatie;
- het risico op doorgifte van data naar landen buiten de EER
- het aantal bekende privacy en security incidenten;
- de samenloop met lopende inkooptrajecten van SURF;
- indicaties dat privacy en/of security zaken niet op orde zijn.

Vervolgstappen

1. Nadat we alle wensen hebben ontvangen bundelen we deze aan de hand van een aantal criteria, zoals:
   - mogelijke samenwerking met andere partijen, zoals het Ministerie van Justitie en Veiligheid en SIVON;
   - het gebruik en de urgentie van de applicatie binnen de sectoren;
   - gesignaleerde issues zoals locatie dataopslag, incidenten bij leveranciers en mogelijke conflicten met inkooptrajecten.
   - de inschatting van de zwaarte van een traject: valt een traject voor een bepaalde leverancier in de categorie klein, midden of groot. Per categorie wordt op basis van de beschikbare capaciteit gekeken hoeveel leveranciers in de komende periode kunnen worden opgepakt.
2. Vervolgens wordt gekeken welke leveranciers in aanmerking komen voor een traject. Dit gebeurt onder andere op basis van een evenredige spreiding van leveranciers die voor de verschillende sectoren relevant zijn.
3. De Leveranciers Compliance Dienstverlening vertaalt deze informatie naar een voorstel voor een kalender: wanneer worden welke trajecten uitgevoerd.
4. Deze lijst wordt voorgelegd aan de regiegroep Cyberveiligheid. Deze regiegroep geeft ons hierop advies.
5. Dit advies leggen we oor aan de CSC-voorzitters, waarna de kalender definitief wordt vastgesteld door de Raad van Bestuur.
6. Communicatie naar de leden over de Leveranciers Compliance kalender 2024.