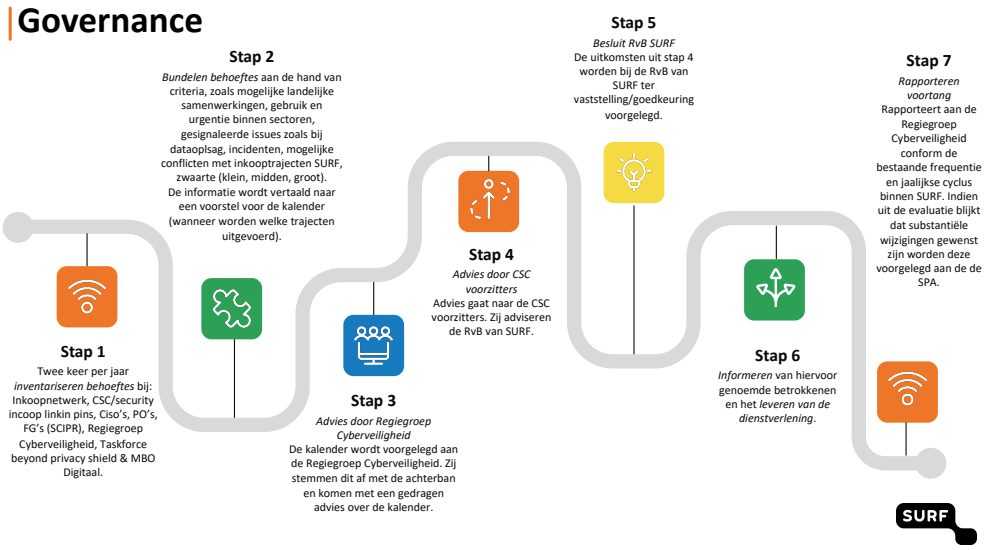
Veelgestelde vragen SURF Vendor Compliance

Vragen over de dienstverlening

Voeren jullie alleen compliance trajecten uit op applicaties waar SURF een overeenkomst mee heeft?

Nee, we voeren trajecten uit op leveranciers/applicaties waarbij binnen de sector behoefte is aan gesprekken over privacy en/of security. Dit hoeven geen partijen te zijn waar we al een overeenkomst mee hebben. We onderhandelen zoveel mogelijk aanpassingen/contractafspraken waarvan de gehele onderwijs- en onderzoekssector kan profiteren. Dit geldt ook als contracten rechtstreeks tussen de instelling en de leverancier worden afgesloten. Een bijkomend voordeel is dat deze trajecten kunnen leiden tot een overeenkomst via SURF, denk bijvoorbeeld aan Zoom.

Hoe wordt er besloten welke trajecten er worden opgepakt/wat is de governance?



Wat is de toegevoegde waarde van deze dienstverlening, aangezien instellingen zelf verantwoordelijk zijn voor het wel/niet inzetten van een applicatie?
We hebben van leden de vraag gekregen of wij namens de sector DPIA's, DTIA's en security checks willen uitvoeren op leveranciers/applicaties die relevant zijn voor het merendeel van de leden. SURF onderhandelt namens de hele sector, waardoor we velen malen sterker staan tegenover leveranciers dan individuele instellingen.

Als we een risicoanalyse hebben uitgevoerd op een leverancier/applicatie gaan we met de leverancier in gesprek over de maatregelen om eventueel gevonden risico's zoveel mogelijk op te lossen. Veel van deze afspraken worden vastgelegd in bijvoorbeeld een standaard verwerkersovereenkomst. Ook worden er instructies gemaakt waarin staat hoe instellingen op een zo privacy en security vriendelijke manier gebruik kunnen maken van de applicatie. Deze instructies worden zoveel mogelijk openbaar gedeeld.

Of jouw instelling daadwerkelijk gebruik maakt van de applicatie is aan de instelling zelf. De instelling heeft de verantwoordelijkheid om te beoordelen of de applicatie/leverancier in te zetten is binnen de eigen processen. Wij verrichten veel voorwerk, maar de instelling moet het zelf toepasbaar maken binnen de eigen organisatie. Je kunt hierbij profiteren van de technische, organisatorische en juridische afspraken die wij voor je geregeld hebben.

Wat zijn de kosten om gebruik te kunnen maken van deze dienstverlening?
De kosten voor het uitvoeren van compliance trajecten wordt bekostigd uit de Basisvergoeding Inkoop en Digitale Platformen (BIDP). De leden hebben goedkeuring gegeven om de SURF Vendor Compliance dienstverlening hierin op te nemen. Vrijwel alle leden betalen deze basisvergoeding, inclusief voor de SURF Vendor Compliance dienstverlening. Er wordt dus op centraal niveau aan de dienst bijgedragen.

Hoe kan ik mijn wensen voor nieuwe compliance trajecten doorgeven?
We pakken gemiddeld acht trajecten per jaar op. Om de behoefte voor de agenda op te halen versturen we twee keer per jaar een uitvraag naar de volgende personen: CISO's, security officers, privacy officers en FG's via het SCIPR-netwerk, contactpersonen software, CSC's, de regiegroep Cyberveiligheid, de Taskforce Beyond Privacy Shield en MBO Digitaal (via het IBP netwerk).

Heb je in de tussentijd wensen, dan kun je deze doorgeven via het inventarisatieformulier. De wensen die wij tussentijds ontvangen worden meegenomen in de volgende update van de kalender.

Heeft het nut om de wensen van mijn instelling door meerdere personen kenbaar te laten maken, of kijken jullie instellingsbreed naar de ontvangen behoefte?
Als er binnen de instelling verschillende behoeften zijn, bijvoorbeeld bij verschillende afdelingen, kun je dit door verschillende personen aan laten leveren. Als dezelfde applicatie meerdere keren wordt genoemd tellen we deze één keer. Alle aangeleverde applicaties per instelling tellen namelijk één keer mee.

Algemene vragen

Waarom moeten er compliance trajecten worden uitgevoerd?
Instellingen maken op grote schaal gebruik van verschillende leveranciers. In veel gevallen verwerken leveranciers persoonsgegevens van de SURF-leden en hun gebruikers. Instellingen zijn volgens de AVG verplicht om hun leveranciers te controleren op hoe zij omgaan met privacy en security. SURF pakt dergelijke compliance trajecten op verzoek van instellingen op. We gaan namens instellingen met leveranciers in gesprek over privacy en/of security en zorgen ervoor dat leveranciers maatregelen nemen om geconstateerde risico's op te lossen. Het loont om dit gezamenlijk namens alle instellingen te doen, door het bundelen van kennis en expertise realiseren we een kostenbesparing, kennisdeling en hebben we een sterkere onderhandelingspositie richting leveranciers.

Wat is een DPIA?
Een DPIA, Data Protection Impact Assessment (DPIA), ook wel een gegevensbeschermingseffectbeoordeling, is een instrument om privacy risico's voor betrokkenen (bijvoorbeeld gebruikers) in kaart te brengen. Vanuit de Algemene Verordening Gegevensbescherming (AVG) is een DPIA noodzakelijk indien er sprake is van grootschalige verwerking van persoonsgegevens of gevoelige persoonsgegevens.

Waarom laat SURF DPIA's uitvoeren?
Via SURF maken de leden gezamenlijk afspraken met ict- en contentleveranciers over de levering en afname van producten en diensten. Zo zorgen de leden gezamenlijk voor schaalgrootte en een efficiënt aanspreekpunt voor leveranciers. Het uitvoeren van risicoanalyses zoals DPIA's zijn hier een onderdeel van. In veel gevallen verwerken leveranciers persoonsgegevens van (werknemers en studenten van) de SURF-leden. Het is daarom belangrijk dat de leveranciers voldoen aan wet- en regelgeving. SURF werkt hierin zoveel als mogelijk samen met samenwerkingspartners zoals SIVON en de overheid. Er zijn samen al meerdere DPIA's uitgevoerd.

Werken SURF en SIVON samen als het over de DPIA's gaat?
Ja, er is een nauwe samenwerking tussen SIVON en SURF. Evenals MBO Digitaal en SURF (en andere samenwerkingspartners zoals het Rijk). Als het even kan werken we samen op de verschillende DPIA's of wisselen informatie uit over de lopende trajecten.

Voor wie is een DPIA toepasbaar?
Iedere instelling moet zelf bepalen in hoeverre de resultaten toepasbaar zijn op de eigen organisatie. De opgeleverde DPIA's kunnen derhalve door iedereen worden gebruikt, ook door organisaties buiten onderwijs en onderzoek, maar moeten altijd worden uitgelegd naar de eigen situatie, processen en omgeving.

Voert SURF de trajecten zelfstandig uit?
In de meeste gevallen werken we samen met samenwerkingspartners zoals de Overheid, SIVON en laten we onderzoeken uitvoeren door externe partijen, zoals Privacy Company.

Waarom zijn de meeste risicoanalyses, zoals DPIA's, in het Engels?
De risicoanalyses zijn in het Engels, omdat de voertaal bij internationale leveranciers Engels is. De resultaten moeten ook voor medewerkers van deze organisaties duidelijk

zijn en niet verkeerd geïnterpreteerd of vertaald worden. Daarnaast zijn ze dan door een brede doelgroep leesbaar.