Samen aanjagen van vernieuwing

Ongeldigverklaring EU-US Privacy Shield en gevolgen voor contracten en inkooptrajecten

Aanbevelingen van SURF aan haar leden

Versie: 1.0
Datum: 6 november 2020

Inhoudsopgave

1 Aanleiding en inleiding 3

2 Wat is het Privacy Shield en wat is de status? 4

3 Wat zijn Standard Contractual Clauses en zijn deze een alternatief voor Privacy Shield? 5

4 Uitwerking van alternatieve routes 6

4.1 Aankomende en lopende aanbestedingsprocedures 6
Route A: Verwerking van alle persoonsgegevens vindt plaats binnen de EER 6
Route B: Verwerking van alle persoonsgegevens binnen de EER is (nog) geen optie 7
4.2 Bestaande contracten 8

5 FAQ en overzicht maatregelen 10

Is het voor instellingen mogelijk om bestaande contracten die gebruik maken van Privacy Shield, te ontbinden? 10
Is het voor instellingen mogelijk om leveranciers die gebruik maken van Privacy Shield, te weren bij nieuwe (nog op te starten) aanbestedingen? 10
Kunnen leveranciers uit de Verenigde Staten worden uitgesloten bij aanbestedingen? 10
Welke mogelijkheden zijn er om in aanbestedingen te zorgen voor een rechtmatige inkoop? 11

6 Betrokken instanties: status en (te verwachten) vervolgstappen 12

1 Aanleiding en inleiding

De Universiteiten (CSC-WO) hebben SURF gevraagd hen te adviseren over de gevolgen van de uitspraak van het Europees Hof van Justitie, waarbij het EU-US Privacy Shield (hierna 'Privacy Shield') ongeldig is verklaard. Wat is de impact van deze uitspraak op lopende contracten en inkooptrajecten?

Dit document bevat praktische aanbevelingen van SURF in het kader van lopende contracten en inkooptrajecten, waarbij doorgifte van persoonsgegevens aan de Verenigde Staten een rol (kunnen) spelen, gericht op toepassing door inkoopteams van de bij SURF aangesloten instellingen.

SURF merkt hierbij op dat de inhoud van dit document een momentopname is, gebaseerd op de stand van zaken zoals die bekend is bij publicatie. Op termijn worden in ieder geval vanuit de Europese toezichthouder aanvullende richtlijnen verwacht naar aanleiding van de uitspraak van het Hof, die kunnen leiden tot gewijzigde inzichten.

SURF is voornemens om toekomstige ontwikkelingen mee te nemen in een Taskforce Privacy Shield, met experts vanuit SURF en de leden. In deze taskforce kunnen ook eventuele aanpassingen aan dit document aan de orde komen. De lezer van dit document doet er dan ook goed aan steeds de meest recente stand van zaken na te vragen bij de taskforce.

Tot slot merkt SURF op dat het om complexe materie gaat, waarbij veel stakeholders zijn betrokken. Bij de toepassing van de aanbevelingen dient daarom steeds beoordeeld te worden of zij passend zijn voor de eigen organisatie, het desbetreffende inkooptraject/de bestaande relatie met de leverancier en of zij aansluiten bij het geheel aan contractuele verplichtingen dat wordt overeengekomen met een leverancier.

2 Wat is het Privacy Shield en wat is de status?

Het Privacy Shield is een overeenkomst tussen de Verenigde Staten de Europese Commissie over de bescherming van persoonsgegevens van EU-burgers in de Verenigde Staten. Op basis van deze overeenkomst en het daarop gebaseerde adequaatheidsbesluit van de Europese Commissie hoeven geen additionele waarborgen getroffen te worden, als persoonsgegevens worden doorgegeven aan een organisatie in de Verenigde Staten die is gecertificeerd onder het Privacy Shield programma.[1]

Het Europees Hof van Justitie (de hoogste rechter van de EU en hierna te noemen 'Hof') heeft nu echter geoordeeld dat de overeenkomst tussen de Verenigde Staten en de Europese Commissie niet voldoende bescherming biedt voor de persoonsgegevens van EU-burgers. De redenen hiervoor zijn:

- De Amerikaanse wetgeving en inlichtingen- en veiligheidsdiensten hebben het recht om gegevens van EU-burgers in te zien en te gebruiken. Dit is niet beperkt tot strikt noodzakelijke gegevens;
- Het ombudsman-mechanisme biedt niet genoeg bescherming wanneer EU-burgers een klacht hebben over de verwerking van hun persoonsgegevens in de Verenigde Staten. Het mechanisme kan de onafhankelijkheid van de ombudsman en diens bevoegdheid om bindende besluiten te nemen niet verzekeren.

Als gevolg van de uitspraak van het Hof, is iedere doorgifte van persoonsgegevens van EU-burgers aan de Verenigde Staten, die plaatsvindt op grond van het Privacy Shield, onrechtmatig.

Om misverstanden te voorkomen, wordt vermeld dat de ongeldigverklaring van het Privacy Shield alleen van belang is voor gevallen waarin persoonsgegevens worden doorgegeven aan de Verenigde Staten. De ongeldigverklaring heeft geen gevolgen voor de doorgifte van andersoortige gegevens.

Voor de volledigheid wordt vermeld dat de uitspraak ook gevolgen kan hebben voor de toepassing van andere doorgiftemechanismen, zoals de Standard Contractual Clauses en de Binding Corporate Rules. Hierop wordt in het volgende hoofdstuk van dit document ingegaan.

[1] De lijst van organisaties die gecertificeerd zijn, is te vinden via https://www.privacyshield.gov/list.

3 Wat zijn Standard Contractual Clauses en zijn deze een alternatief voor Privacy Shield?

- Standard Contractual Clauses (SCC's) zijn door de Europese Commissie vastgestelde modelcontracten, met betrekking tot de bescherming van gegevens bij een doorgifte naar landen buiten de EU of de EER. Het afsluiten van deze model contracten zijn een manier om bij een doorgifte naar landen zoals hierboven genoemd, een voldoende beschermingsniveau te bewerkstelligen.

- Standard Contractual Clauses zijn niet ongeldig verklaard in de uitspraak van het Europese Hof van Justitie.

- Voor de doorgifte van persoonsgegevens op basis van SCC's is echter een analyse per geval noodzakelijk, van de omstandigheden rond de doorgifte en de aanvullende maatregelen. De vraag die beantwoord moet worden, is of bij de doorgifte een passend beschermingsniveau kan worden gegarandeerd.

- Voor een doorgifte naar de VS is het zeer twijfelachtig of een passend beschermingsniveau kan worden geboden, wanneer dit via SCC's plaatsvindt. Dit gelet op de beoordeling van het Hof, van het huidige beschermingsniveau in de VS.

- Desalniettemin zijn SCC's momenteel vaak het enige praktisch beschikbare doorgifte mechanisme voor de doorgifte van persoonsgegevens naar de VS. Er zijn weinig andere opties[2].

Advies van SURF aan haar leden:
Neem tekst in aanbestedingen en overeenkomsten op, die leveranciers verplicht om actief en tijdig mee te werken aan maatregelen die nodig zijn om aanvullingen op of alternatieven voor Standard Contractual Clauses door te voeren. Via de Taskforce zullen hiervoor voorbeeldbepalingen worden aangedragen.

[2] Een alternatief mechanisme voor doorgifte zijn de Binding Corporate Rules (BCR). Binnen internationale organisaties kan doorgifte van persoonsgegevens plaats vinden tussen de verschillende vestigingen op basis van goedgekeurde interne bindende bedrijfsvoorschriften, waarin de waarborgen voor de bescherming van persoonsgegevens zijn vastgelegd. Naast dat er maar beperkt gebruik wordt gemaakt van BCR, ligt het voor de hand dat in deze situatie dezelfde vragen gesteld dienen te worden als bij de SCC's. Ook de specifieke uitzonderingen van artikel 49 van de AVG zullen maar in weinig gevallen werkbaar zijn. Het biedt geen oplossing voor structurele systematische doorgifte.

4 Uitwerking van alternatieve routes

4.1 Aankomende en lopende aanbestedingsprocedures

In deze paragraaf wordt beschreven welke routes kunnen worden gevolgd in aankomende en lopende aanbestedingsprocedures. Hierbij wordt een onderscheid gemaakt tussen twee mogelijke routes:

- Route A: alle persoonsgegevens worden binnen de EER verwerkt, waardoor de uitspraak van het Hof geen rol speelt;
- Route B: (een gedeelte van) de persoonsgegevens wordt niet binnen de EER verwerkt, waardoor rekening moet worden gehouden met de gevolgen van de uitspraak van het Hof.

Route A: Verwerking van alle persoonsgegevens vindt plaats binnen de EER

- *Aankomende aanbestedingsprocedures*
  Neem als eis op dat alle verwerkingen van persoonsgegevens plaats moeten vinden binnen de EER. Via de Taskforce zullen hiervoor voorbeeldbepalingen worden aangedragen. Met de uitspraak van het Europese Hof van Justitie is er voldoende grond om een dergelijke eis op te nemen. Het is niet nodig om dat uitgebreid te motiveren. Eventueel kan nog gekozen worden om ook verwerkingen toe te staan in landen waarvoor een adequaatheidsbesluit is genomen, zoals bedoeld in artikel 45 AVG. Dit maakt het risico minder groot, op het kwalificeren van de eis als zijnde niet-proportioneel.[3]

  De eis dient betrekking te hebben op alle verwerkingen, door de leverancier en door de subverwerkers die in de gehele keten van verwerkingen worden ingeschakeld. Daarnaast dient de eis betrekking te hebben op alle verwerkingen. Het beperken van de eis tot alleen de opslag van gegevens binnen de EER, heeft niet het gewenste effect zolang er toegang is of kan zijn tot de gegevens vanaf buiten de EER. Zeker bij organisaties met een moedermaatschappij, komt het bijvoorbeeld veelvuldig voor dat de moedermaatschappij betrokken is bij een deel van de levering van de dienst of op zijn minst toegang heeft tot de persoonsgegevens. Bij organisaties met een Amerikaanse moedermaatschappij betekent dit, dat hoewel de persoonsgegevens in Europa zijn opgeslagen, nog steeds een doorgifte aan de Verenigde Staten plaatsvindt.

  Advies: Laat leveranciers in hun inschrijving aangeven in welke landen de verwerkingen van persoonsgegevens plaatsvinden (door henzelf en binnen de gehele keten van subverwerkers die worden ingeschakeld), met daarbij een beschrijving van de aard van de verwerking. Leveranciers die aangeven dat persoonsgegevens buiten de EER worden verwerkt, kunnen op grond van de aanbestedingseis worden uitgesloten.

[3] Hierbij wordt wel opgemerkt dat er altijd een risico is dat een adequaatheidsbesluit wordt ingetrokken of ongeldig verklaard (zoals dit bijvoorbeeld in het geval van het op het Privacy Shield gebaseerde adequaatheidsbesluit voor de Verenigde Staten is gebeurd).

- *Lopende aanbestedingsprocedures*
  Het is toegestaan om wijzigingen aan te brengen in een lopende aanbesteding, zolang als dit geen *wezenlijke* wijzigingen betreft. Echter, het wijzigen van de toegestane lijst van locatie van verwerkingen van persoonsgegevens raakt de kring van gegadigden, is daarmee een wezenlijke wijziging en in verband daarmee kan in een lopende aanbesteding geen additionele eis ten aanzien van de locatie van verwerkingen van persoonsgegevens worden gesteld. De enige optie is de tender opnieuw te starten en dan bovengenoemde eis over de locatie van de verwerkingen van persoonsgegevens toe te voegen.

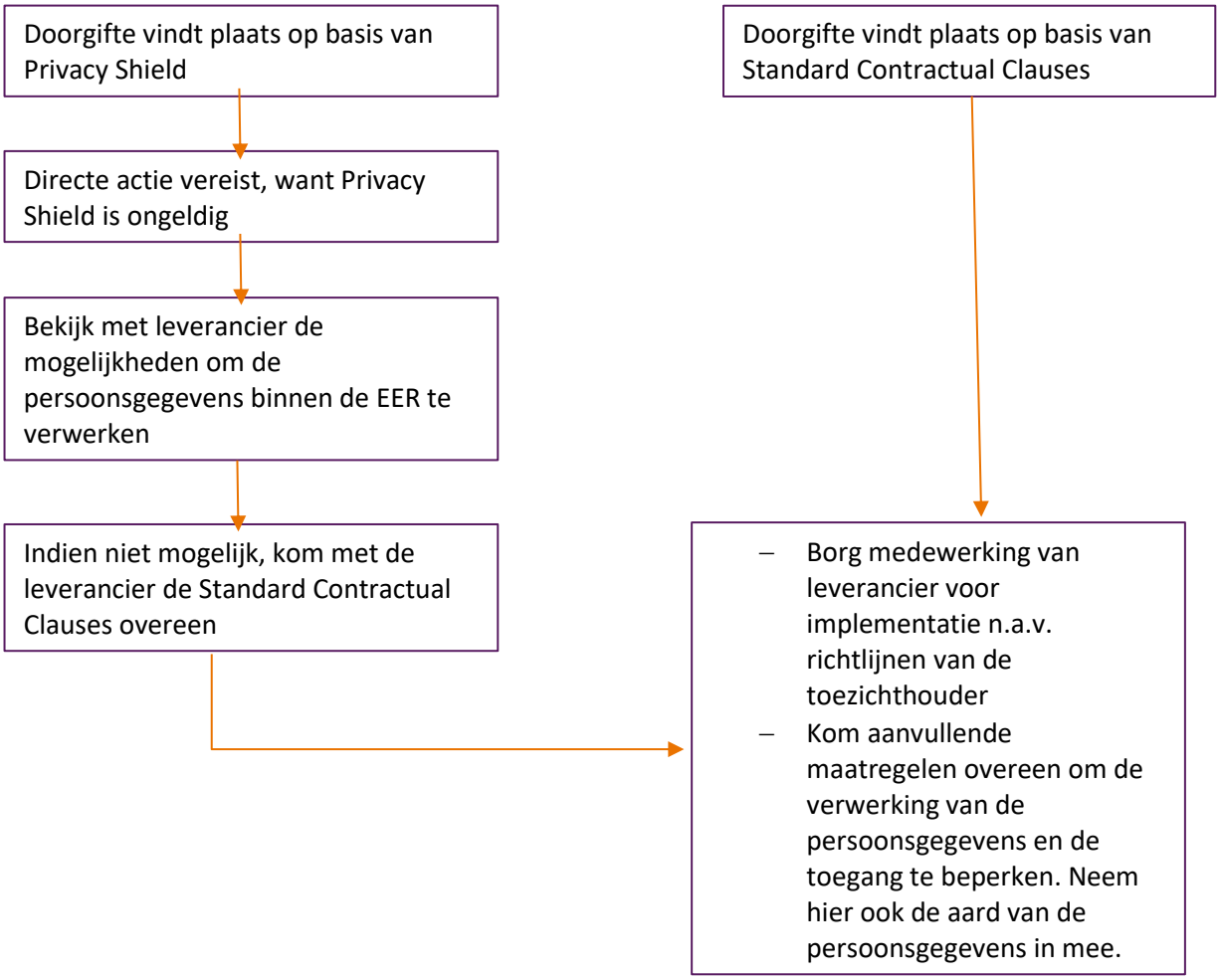
Route B: Verwerking van alle persoonsgegevens binnen de EER is (nog) geen optie

- *Aankomende aanbestedingsprocedures*
  Voor aankomende aanbestedingsprocedures is het belangrijk in de aanbestedingsstukken te borgen dat de leverancier:
  - Moet voldoen aan de geldende wet- en regelgeving van tijd tot tijd; en
  - Actief moet meewerken aan het implementeren van aanvullende maatregelen ten aanzien van de inrichting van zijn dienst en/of de inhoud van de verwerkersovereenkomst en/of de SCC's, voor zover deze maatregelen voortvloeien uit de door de Europese of Nederlandse toezichthouder in verband met de rechtmatigheid van doorgiften buiten de EER van tijd tot tijd gepubliceerde richtlijnen.

  Via de Taskforce zullen hiervoor voorbeeldbepalingen worden aangedragen. Door deze bepalingen op te nemen in de aanbestedingsstukken, wordt enerzijds zeker gesteld dat een leverancier al tijdens de verificatieprocedure kan worden aangesproken op de wijze waarop de doorgifte naar buiten de EER wordt geregeld en anderzijds dat dit gedurende de hele looptijd van de overeenkomst kan worden gedaan, ook als er nieuwe richtlijnen worden gepubliceerd. Als bij de verificatie dus bijvoorbeeld blijkt dat de leverancier nog steeds het Privacy Shield als doorgiftemechanisme wil hanteren, kan deze leverancier worden uitgesloten.
  Daarnaast is van belang te inventariseren in hoeverre nu al aanvullende technische eisen kunnen worden gesteld, waardoor de feitelijke toegang tot de persoonsgegevens vanaf buiten de EER wordt beperkt. Denk hierbij aan eisen op het gebied van encryptie van de persoonsgegevens die worden opgeslagen in de dienst van de leverancier. Deze technische maatregelen kunnen worden opgenomen in de aanbestedingsstukken.
- *Lopende aanbestedingsprocedures*
  Voor lopende aanbestedingsprocedures geldt dat je geen wezenlijke wijzigingen mag doorvoeren. Dit heeft tot gevolg dat geen aanvullende technische eisen meer mogen worden gesteld. Het toevoegen van bepalingen waarmee de naleving van wet- en regelgeving wordt geborgd, dient niet te worden gekwalificeerd als een wezenlijke wijziging. Voor zover deze eis dus nog niet is opgenomen, kunnen deze alsnog worden opgenomen. Leveranciers waarvan tijdens de verificatieprocedure blijkt dat zij het Privacy Shield als doorgiftemechanisme willen gebruiken, kunnen op dat moment worden uitgesloten.

4.2 Bestaande contracten

Hierna volgt een overzicht van de stappen die genomen moeten worden voor bestaande contracten, afhankelijk van het huidige doorgiftemechanisme dat wordt gebruikt voor de doorgifte van persoonsgegevens aan de Verenigde Staten:



Hierbij zijn de volgende aandachtspunten van toepassing:

- Beperking van verwerking tot de EER: de praktijk leert dat veel leveranciers, die nu gebruik maken van het Privacy Shield als doorgiftemechanisme, niet in staat zijn om een oplossing te leveren waarbij alle verwerkingen ineens alleen binnen de EER plaatsvinden. Voor zover leveranciers de oplossing bieden dat objectdata binnen de EER worden opgeslagen, moet nog kritisch gekeken worden naar eventuele andere verwerkingen (dan opslag) die plaatsvinden en door welke partijen deze plaatsvinden. Zeker bij organisaties met een moedermaatschappij, komt het bijvoorbeeld veelvuldig voor dat de moedermaatschappij betrokken is bij een deel van de levering van de dienst of op zijn minst toegang heeft tot de persoonsgegevens. Bij organisaties met een Amerikaanse moedermaatschappij betekent dit, dat hoewel de persoonsgegevens in Europa zijn opgeslagen, nog steeds een doorgifte aan de Verenigde Staten plaatsvindt.

- Borgen van medewerking van de leverancier ten aanzien van implementatie maatregelen. Let hierbij op dat de contractuele verplichting die met de leverancier wordt overeengekomen, ook voldoende afdwingbaar is in de praktijk. Deze afdwingbaarheid komt tot uiting in bijvoorbeeld de aansprakelijkheidsbepalingen, eventuele boetebepalingen en de mogelijkheden tot ontbinding van de overeenkomst. Via de Taskforce zullen hiervoor voorbeeldbepalingen worden aangedragen.
- Aanvullende technische maatregelen om de toegang tot de persoonsgegevens vanaf buiten de EER te beperken: denk hierbij aan maatregelen als encryptie van de persoonsgegevens die bij de leverancier zijn opgeslagen. Neem dergelijke technische maatregelen op in de overeenkomst. Ook dit onderdeel zal via de Taskforce nader worden uitgewerkt.

5 FAQ en overzicht maatregelen

Is het voor instellingen mogelijk om bestaande contracten die gebruik maken van Privacy Shield, te ontbinden?

Het afscheid kunnen nemen van een leverancier die gebruik maakt van het Privacy Shield als doorgiftemechnisme, dient van geval tot geval te worden beoordeeld. De regeling in de desbetreffende overeenkomst voor gevallen waarin de leverancier niet voldoet aan wet- en regelgeving, zal hiervoor leidend zijn.

Is het voor instellingen mogelijk om leveranciers die gebruik maken van Privacy Shield, te weren bij nieuwe (nog op te starten) aanbestedingen?

Ja.
Het Hof heeft aangegeven dat de Privacy Shield geen geldig doorgiftemechanisme vormt. Een leverancier die hiervan gebruikmaakt, mag worden uitgesloten, als de aanbestedingsstukken hierin voorzien – zie hiervoor paragraaf 4.1.

Kunnen leveranciers uit de Verenigde Staten worden uitgesloten bij aanbestedingen?

Nee.
Dit is niet toegestaan op grond van de WTO, waarin is opgenomen dat Amerikaanse bedrijven bij aanbestedingen niet mogen worden gediscrimineerd ten opzichte van Europese bedrijven. Het is dus niet mogelijk om leveranciers, enkel en alleen op grond van hun vestigingsadres, uit te sluiten. De beperking moet worden gezocht in de locaties waar de verwerkingen plaats mogen vinden – zie hiervoor paragraaf 4.1.

Welke mogelijkheden zijn er om in aanbestedingen te zorgen voor een rechtmatige inkoop?

Instrument	Is toepassing mogelijk in een nieuwe aanbesteding?	Is toepassing mogelijk in een al lopende aanbesteding?	Is toepassing mogelijk in lopende overeenkomsten (aanbesteed)	Is toepassing mogelijk in lopende overeenkomst (niet aanbesteed)
1. Bepaling opnemen, of nakoming verlangen van een bepaling, dat leverancier voldoet aan privacy wetgeving, middels: a. verklaring van leverancier dat hij voldoet b. verificative c. certificaat d. audit	Ja	Ja	Ja	Ja, indien leverancier hiermee instemt
2. Eis stellen dat verwerking binnen de EER en Zwitserland moet plaatsvinden.	Ja	Nee[4]	Nee[1]	Ja, indien leverancier hiermee instemt
3. Sancties op niet naleven 1. of 2.	Ja[5]	Nee, geen nieuwe.[6]	Nee, geen nieuwe.[7]	Ja, indien leverancier hiermee instemt
4. SSC (zie eerdere opmerkingen in dit document, over beperkingen)	Ja	Nee[8]	Nee[9]	Ja, indien leverancier hiermee instemt
5. Encryptie	Ja	Nee[10]	Nee[11]	Ja, indien leverancier hiermee instemt

	mag
	hangt ervan af
	mag niet

[4] Dit zal snel als een wezenlijke wijziging worden gezien. Mogelijke escape: aangeven dat leverancier zich aan de privacywetgeving moet houden en dit als optie voorstellen aan leverancier, zodat deze daaraan kan voldoen. Dan mag dit vermoedelijk wel in veel gevallen.

[5] Hiervoor geldt wel een proportionaltiteitstoets

[6] Waarschijnlijk wel toegestaan: de leverancier *vragen* om boetes e.d. op zich te nemen. Maar daar hij kan niet toe worden verplicht.

[7] Waarschijnlijk wel toegestaan: de leverancier *vragen* om boetes e.d. op zich te nemen. Maar daar hij kan niet toe worden verplicht.

[8] Zie voetnoot 3

[9] Zie voetnoot 3

[10] Zie voetnoot 1.

[11] Zie voetnoot 1.

6 Betrokken instanties: status en (te verwachten) vervolgstappen

De toezichthouder: de Autoriteit Persoonsgegevens en de European Data Protection Board

- De Nederlandse Autoriteit Persoonsgegevens (AP) is vooralsnog stil op dit onderwerp en verwijst naar de European Data Protection Board (EDPB). Binnen de EDPB werken de toezichthoudende autoriteiten van andere Europese landen samen

- De verwachting is dat de EDPB meer richting zal geven, in de vorm van richtsnoeren gericht op de aanvullende maatregelen. Als eerste actie heeft de EDPB een FAQ over de uitspraak gepubliceerd.

- De EDPB heeft laten weten geen ruimte te zien voor een transitieperiode waarin nog niet direct handhavend wordt opgetreden tegen doorgifte gebaseerd op het Privacy Shield.

- Er zijn momenteel echter nog geen organisaties door de AP aangesproken op het feit dat zij niet zouden voldoen aan wet- en regelgeving, door de ongeldigverklaring van Privacy Shield.

Het Rijk

Ook de overheid wacht af op wat de European Data Protection Board (EDPB) gaat doen en noemt het van groot belang dat er een nieuw adequaatheidsbesluit komt, dat de door het Hof geconstateerde gebreken in het Privacy Shield repareert. Dit blijkt uit de antwoorden op de Kamervragen en de reactie op de brief van NL-digitaal.

> https://www.rijksoverheid.nl/documenten/kamerstukken/2020/10/12/antwoorden-kamervragen-inzake-het-bericht-eu-hof-amerikaanse-privacybescherming-onvoldoende
>
> https://www.rijksoverheid.nl/documenten/kamerstukken/2020/09/30/tk-reactie-op-de-brief-van-nl-digitaal-over-de-gevolgen-van-schrems-ii

Europese Commissie

- Vaststelling van een adequaatheidsbesluit is een bevoegdheid van de Europese Commissie. De Commissie is in gesprek met de VS over de mogelijkheden voor een nieuw besluit.

- Nieuwe afspraken maken zal lastig zijn. De EC moet de uitspraak van het Hof respecteren. De bezwaren die het Hof heeft genoemd met betrekking tot het beschermingsniveau in de VS, zijn niet eenvoudig weg te nemen.

- De verwachting is dat er niet op korte termijn een nieuw adequaatheidsbesluit zal zijn. Op zijn vroegst in de tweede helft van 2021.

Instellingen (leden van SURF)

- Instellingen zijn verplicht zich in te spannen om te voldoen aan wet- en regelgeving; om compliant te zijn.
- SURF richt een Taskforce Privacy Shield op, om hier gezamenlijk aan te werken. Door zich hierbij aan te sluiten, tonen instellingen (richting de AP) aan dat zij zich die inspanning getroosten.