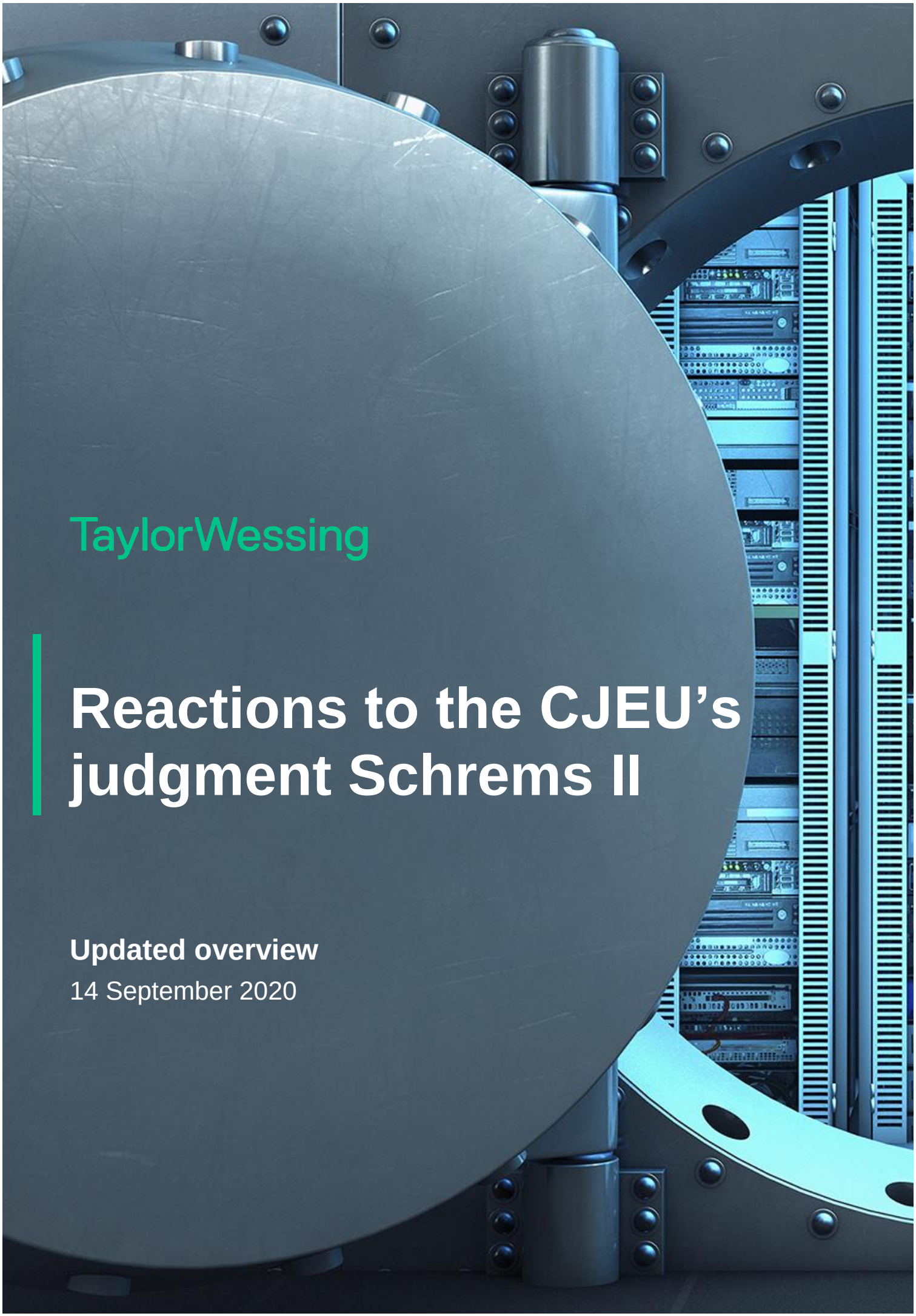

TaylorWessing

Reactions to the CJEU's judgment Schrems II

Updated overview

14 September 2020

The following overview summarises the statements made by supervisory authorities and EU and US institutions up to now (alphabetical order by country code; EU for institution at EU level).

Country code	Supervisory authority	Statement
BG	**Комисия за защита на личните данни** Link [en]	The Bulgarian Commission for Personal Data Protection has acknowledged that future data transfers to the US have to be based on other safeguards under the GDPR – eg Binding Corporate Rules (BCR) or EU Standard Contractual Clauses (SCC). In addition, the Bulgarian Commission for Personal Data Protection provides a link to the EDPB's FAQ.
CH	**Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter** Link [en]	The Swiss Federal Data Protection and Information Commissioner (FDPIC) considers that the CJEU's judgment is not directly applicable to Switzerland. It is anticipated that the FDPIC will provide a more comprehensive opinion in due course.
CY	**Γραφείο Επιτρόπου Δεδομένων Προσωπικού Χαρακτήρα** Link [el]	The Cyprian Office of the Commissioner for Personal Data Protection considers that SCC remain valid, but companies must take into account the surveillance practices of the third country and implement additional measures, where necessary. The Cyprian Commissioner for Personal Data Protection has not indicated what she means by "additional measures". She further explains that where an adequate level of data protection cannot be ensured, data transfers must be suspended or terminated. For further information, she refers to the EDPB's statement and FAQ.
CZ	**Úřad pro ochranu osobních Ùdajů** Press release: Link [cs] Statement: Link [cs] FAQ: Link [cs]	The Czech Office for the Protection of Personal Data considers that data transfers to the US cannot be based on the EU-US Privacy Shield anymore. In general, the use of SCC could continue, but the data exporter must examine if the safeguards provided by SCC actually provide an equivalent level of data protection as in the EU. In this context, the data exporter must take into account the circumstances of the data transfer, the country of the data importer and the relevant elements of the third country's legal system. With respect to data transfers to the US, the Czech Office for the Protection of Personal Data considers that the CJEU has found that the US does not provide an adequate level of data protection of EU data subjects. In view of this, data controllers who transfer personal data to the US based on SCC must discuss the specific implications of the CJEU's judgment with the data importer and seek solutions in form of additional measures. As examples, it explicitly mentions the

		retention of metadata within the EU and "encryption without backdoors". Apart from that, it points out the data controller's obligation to inform the data subject in a transparent manner about the data transfer, the conditions of data protection and the risks involved. Finally, the Czech Office for the Protection of Personal Data has provided answers to FAQ predominantly comprising the data transfer to third countries in general.
DE	**Datenschutzkonferenz (DSK)** Link [de]	The German Data Protection Conference (DSK) expresses its belief that the CJEU's judgment has strengthened the data protection rights of EU citizens and considers that the EU-US Privacy Shield cannot be relied upon and that such data transfers must be stopped immediately. In general, the use of SCC could continue, but the data exporter and importer must assess whether the third country offers an adequate level of data protection. Where this is not the case (eg the US), additional measures must be taken. These additional measures should not be undermined by the rules and regulations of the third country. Furthermore, the DSK points out that the findings of the CJEU's judgment applied to all appropriate safeguards in the meaning of Art. 46 GDPR, in particular BCR. Where necessary, they also had to be accompanied by additional measures. The DSK considers that only data transfers to the US based on derogations pursuant to Art. 49 GDPR can be used without further action. The DSK advises data controllers who continue to transfer personal data to the US or other third countries to immediately verify whether they comply with the conditions above. Furthermore, the DSK expresses its belief that the CJEU has given the supervisory authorities a key role when it comes to further decisions on the data transfer to third countries. The German supervisory authorities are coordinating their respective approaches within the EDPB and will provide further guidance in the future. Finally, the DSK provides a link to the EDPB's FAQ.
DE	**Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit** Link [en]	The German Federal Commissioner for Data Protection and Freedom of Information considers that data transfers between the EU and the US remain possible. He wants to advise companies on the transition from the EU-US Privacy Shield to other safeguards. He also believes that the supervisory authorities have been strengthened and stresses that data transfers must be stopped if they do not meet the requirements set by the CJEU.
DE	**Berliner Beauftragte für Datenschutz und Informationsfreiheit** Link [en]	The Berlin Commissioner for Data Protection and Freedom of Information welcomes that the CJEU has clarified that data exports are not only about economics, but also that fundamental human rights must be a priority. The "hour of digital independence for Europe" had now come. In addition,

		she considers the CJEU's judgment as a challenge to prohibit inadmissible data transfers to third countries. Besides the US, she explicitly mentions Russia, China and India. She further points out that companies can be liable for damages vis-à-vis data subjects if they transfer personal data to third countries in an inadmissible way.
DE	**Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit** Link [de]	The Hamburg Commissioner for Data Protection and Freedom of Information welcomes the CJEU's judgment. He stresses that the US has not made any significant improvements after the invalidated Safe Harbor Agreement. He argues that the CJEU's stance on SCC as an appropriate instrument for data protection is inconsistent. He believes that the supervisory authorities should jointly develop a strategy on how to deal with international data transfers and sees "difficult times" ahead for them.
DE	**Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz** Press release: Link [de] FAQ: Link [de]	The State Commissioner for Data Protection and Freedom of Information of Rhineland-Palatinate believes that the CJEU's judgment has strengthened the rights of data subjects, but also sees "hard work" ahead for affected companies. He considers that data transfers to third countries must be suspended if local law is incompatible with the GDPR. He further points out the need for coordination between the supervisory authorities. Subsequently, he also compiled a list of answers to FAQ. Therein, he considers that data controllers who based their data transfers to the US on the EU-US Privacy Shield must switch to other safeguards in the meaning of Art. 46 GDPR. Where this is not possible, the data transfer must be suspended and personal data already transferred must be reclaimed. The use of SCC could generally continue, but the data exporter must assess whether the third country's legal framework provides an adequate level of data protection. Where this is not the case (eg the US), additional measures must be taken. In this context, he questions if such additional measures are in fact possible for data transfers to the US and at what threshold the supplement of additional measures requires approval by the competent supervisory authority.
DE	**Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit** Link [de]	The Thuringian State Commissioner for Data Protection and Freedom of Information is not surprised that the CJEU has invalidated the EU-US Privacy Shield. He welcomes the CJEU's "clear finding that the ombudsman mechanism [of the US] does not meet the EU's legal safeguards". He questions whether "SCC can be filled with life" in the future. In his view, the European supervisory authorities are now being called upon to ensure that personal data is transferred to the US in compliance with data protection regulations.
DE	**Landesbeauftragter für Datenschutz und**	In an initial interview with the German newspaper "FAZ", the State Commissioner for Data Protection and Freedom of

	Informationsfreiheit Baden-Württemberg FAZ: Link [de] Press release: Link [de] Orientation guide: Link [de]	Information of Baden-Württemberg welcomes the CJEU's attempts to establish a worldwide level of data protection that is on the same level as the GDPR. Simultaneously, he questions whether or not the CJEU is overestimating the influence of the EU. If the EU were to strictly prevent the data transfer to the US, this would also result in massive damage to the EU. In his subsequent press release and orientation guide, he considers that the CJEU's judgment was accurate, as the EU-US Privacy Shield did not effectively and sufficiently protect EU citizens. However, the CJEU's judgment also put EU companies in a nearly unsolvable situation. If they could not convince US service providers (eg Microsoft, Zoom etc.) to effectively prevent data access by US authorities, they would no longer be allowed to use such service providers. Although a change in US law would be the ideal outcome, it was unlikely that the CJEU's "domino game" will be successful triggering the desired change in US security policy. Nevertheless, he points out that the CJEU's judgment will be enforced by supervisory authorities taking into account "the principle of proportionality". In his view, a particular focus will lie on the question whether there are viable alternatives to data transfers to the US. If a company could not convince him that the service provider is irreplaceable in the short or medium term, the data transfer must be prohibited. With respect to irreplaceable service providers, he is still working on solutions. In his orientation guide, the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg provides further guidance on how to proceed. In particular, he describes the conditions under which personal data can still be transferred to the US (or other third countries) based on SCC. He mentions encryption and anonymization of personal data, but points out that in most cases these additional measures will not be sufficient to justify data transfers to the US. In this case, data exporters should – in order to at least demonstrate their willingness to act in accordance with the law – contact the respective data importers and implement a number of additions to the SCC specified in the FAQ.
DE	**Der Hessische Beauftragte für Datenschutz und Informationsfreiheit** Link [de]	The Hessian State Commission for Data Protection briefly informs about the invalidity of the EU-US Privacy Shield. Furthermore, it published the DSK's statement and refers to EDPB's statement.
DE	**Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern** Link [de]	The State Commissioner for Data Protection and Freedom of Information of Mecklenburg-Western Pomerania briefly considers the CJEU's judgment. In his view, the options available for data exporters are the same as they were five years ago when the Safe Harbor Agreement was invalidated (ie SCC, BCR and individual agreements). Furthermore, he refers to the DSK's and EDPB's statements.

DE	**Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen** Link [de]	The North Rhine-Westphalian State Commission for Data Protection and Freedom of Information briefly summarises the CJEU's judgment. In its view, SCC may still be used, however, the contracting parties have to assess for themselves, whether SCC are sufficient alone or need to be accompanied by additional measures. In particular, this shall apply if the third country provides an insufficient level of data protection. Where SCC are not complied with in the respective third country, the data exporter must suspend the data transfer or at the very least inform the competent supervisory authorities. According to the North Rhine-Westphalian State Commission for Data Protection and Freedom of Information, German and European supervisory authorities are working together in order to understand and enforce the CJEU's judgment uniformly. As regards the question of what additional measures could be taken, it does not provide further information. Rather, it refers to the EDPB, which currently examines what these additional measures could consist of.
DK	**Datatilsynet** Link [da]	The Danish Data Protection Agency provides a short summary of the CJEU's judgment and refers to the EDPB's statement for a detailed analysis.
EE	**Andmekaitse Inspektsioon** Link [et]	The Estonian Data Protection Inspectorate gives a short summary of the CJEU's judgment. In its view, SCC remain a valid alternative. However, it is for the contracting parties to assess whether or not the third country offers an adequate level of data protection. If the protection of personal data cannot be ensured, the data transfer must be suspended or another appropriate safeguard must be found. However, the Estonian Data Protection Inspectorate does not elaborate further on such appropriate safeguards. Further, it refers to the EDPB's FAQ.
ES	**Agencia Española de Protección de Datos (AEPD)** Link [es]	The Spanish Data Protection Agency (AEPD) briefly informs about the CJEU's judgment. The AEPD refers to the EDPB's statement and explains that it will continue working with the other European supervisory authorities in order to find a common and consistent approach to apply the CJEU's judgment within the EU.
EU	**European Data Protection Board (EDPB)** Statement: Link [en] FAQ: Link [en] Plenary session: Link [en]	In its initial statement, the EDPB notes that the CJEU refers to flaws in the EU-US Privacy Shield, which the EDPB had already pointed out. It expresses its desire to support the European Commission in concluding a legally compliant agreement with the US. In addition, the EDPB wants to develop measures that data exporters can implement to ensure the required level of data protection. However, it also draws attention to the obligations contained in SCC and stresses that the supervisory authorities are obliged to prohibit data transfers that do not meet the set requirements.

		The EDPB also provided answers to FAQ, which it aims to further develop and complement as it continues to assess the CJEU's judgment. In the FAQ, the EDPB points out that the threshold set by the CJEU applies to all appropriate safeguards pursuant to Art. 46 GDPR and not only to data transfers to the US, but any third country. Consequently, companies transferring personal data to the US or any other third country based on SCC or BCR have to assess whether the level of data protection required by the GDPR is met within the respective third country in order to determine if the guarantees provided by SCC or BCR can be complied with in practice. Where this is not the case, additional measures must be implemented. It is in the primary responsibility of the data exporter and importer to assess on a case-by-case basis what these additional measures could consist of. These additional measures could be of a legal, technical of organisational nature. In this context, the EDPB also points out that the law of the third country must not impinge on such additional measures in order to ensure their effectiveness. Finally, the EDPB has created a taskforce, which is looking into complaints that have been lodged with the EU supervisory authorities due to the implications of the CJEU's judgment.
EU	**European Data Protection Supervisor (EDPS)** Link [en]	The EDPS welcomes that the CJEU's judgment emphasises the importance of a high level of protection for personal data transferred to third countries. At the same time, the EDPS hopes that the US will soon achieve a level of data protection equivalent to the EU. Based on the CJEU's judgment, the EDPS is also reviewing the agreements that EU institutions have concluded. In this context, the EDPS explicitly mentions Microsoft.
EU	**European Commission** Link [en]	In the European Commission's opening remarks at the press conference following the CJEU's judgment, Vice-President Věra Jourová and Commissioner for Justice Didier Reynders both stressed the importance of data protection and declared that they will do everything to comply with the CJEU's judgment. They welcomed that the CJEU confirmed that SCC remain a valid tool for data transfers to third countries, meaning that transatlantic data transfers could continue. They emphasised that the European Commission is not starting from scratch and had already been working intensively to update the toolbox for international data transfers. In particular, this included a modernisation of SCC, which will be finalised in due course. The European Commission wants to work closely with its US counterparts, the EDPB and the national supervisory authorities to develop a strengthened and durable data transfer mechanism.

FI	**Tietosuojavaltuutetun toimisto** 1st Press release: Link [fi] 2nd Press release: Link [fi]	The Finnish Office of the Data Protection Ombudsman briefly informs about the CJEU's judgment and provides a summary of the EDPB's statement.
FR	**Commission Nationale de l'Informatique et des Libertés (CNIL)** Link [en]	The French National Commission for Information Technology and Civil Liberties (CNIL) acknowledges the CJEU's judgment. The CNIL confirms that it is – together with its European counterparts – conducting a precise analysis on the consequences of the CJEU's judgment. The CNIL also published the EDPB's FAQ on its website.
HR	**Agencija za zaštitu osobnih podataka** Link [hr]	The Croatian Agency for Personal Data Protection refers to the EDPB.
IE	**Data Protection Commission (DPC)** Link [en]	The Irish Data Protection Commission (DPC) welcomes the CJEU's judgment, as it confirms its concerns about data transfers to the US. The DPC states that the CJEU rules that SCC are, in principle, valid, although it is clear that, in practice, the application of the SCC transfer mechanism to data transfers to the US is now questionable. This issue requires further and careful examination, not least because assessments will need to be made on a case-by-case basis. The DPC also acknowledged the central role that it, together with its fellow supervisory authorities across the EU, must play in the area of data transfers. The DPC confirmed it is working on a common position with its European colleagues to "give meaningful and practical effect to [the CJEU's] judgment".
IS	**Persónuverndar** Link [is]	The Icelandic Data Protection Authority summarises the CJEU's judgment and provides links to the EDPB's statement and FAQ.
IT	**Garante per la protezione dei dati personali** Link [it]	The Italian Data Protection Authority briefly summarises the CJEU's judgment and refers to the EDPB.
LI	**Datenschutzstelle Fürstentum Liechtenstein** Link [de]	The Data Protection Office of Liechtenstein provides a short summary of the CJEU's judgment and considers that companies must use other appropriate safeguards pursuant to Art. 46 GDPR, until the EU and the US reach a new agreement on the transfer of personal data. Further, it refers to the EDPB's FAQ.
LT	**Valstybinė duomenų apsaugos Inspekcija** Link [lt]	The Lithuanian State Data Protection Inspectorate briefly summarizes the CJEU's judgment and points out that it is assessing the decision within the EDPB.

LU	**Commission nationale pour la protection des données (CNPD)** Link [en]	The Luxembourg Data Protection Authority (CNPD) welcomes the CJEU's judgment and considers that SCC remain valid, but that the data exporter and importer are obliged to take into account the circumstances of the data transfer. Where applicable, the data importer has to inform the data exporter of any inability to comply with SCC or additional measures that the parties have agreed upon. The data exporter then, in turn, is obliged to suspend the data transfer or terminate the contract with the data importer. Further, the CNPD refers to the EDPB's statement and FAQ.
MT	**Office of the Information and Data Protection Commissioner** Link [en]	The Maltese Office of the Information and Data Protection Commissioner provides a short summary of the CJEU's judgment and refers to the EDPB's FAQ.
NL	**Autoriteit Persoonsgegevens** Link [nl]	The Dutch Data Protection Authority (AP) briefly summarises the CJEU's judgment and points out that the data transfer to the US based on the EU-US Privacy Shield is no longer possible. For further guidance, the AP considers that the EDPB is currently examining the practical consequences of the CJEU's judgment as well as possible next steps. In particular, the EDPB will provide guidance on additional measures in due course. The AP also refers to the EDPB's statement and FAQ.
NO	**Datatilsynet** 1st Press release: Link [no] 2nd Press release: Link [no]	The Norwegian Data Protection Authority published a detailed statement, which includes guidance on how companies should react. It points out that once the data exporter has been notified by the data importer that it is unable to comply with the obligations set out in SCC or BCR, the data exporter must either implement additional measures or stop the data transfer. The Norwegian Data Protection Authority acknowledges that there was great uncertainty as to what kind of additional measures can be taken if the prevailing local (surveillance) regulations of the third country are in conflict with the SCC. In this case, it would most likely not be possible to transfer personal data to such third countries in practice. Accordingly, the Norwegian Data Protection Authority concludes that it is "very challenging or impossible" to find additional measures which would allow the data transfer to the US to continue. For further information, it refers to the EDPB's FAQ.
PL	**Urząd Ochrony Danych Osobowych (UODO)** Link [pl]	The Polish Personal Data Protection Office (UODO) summarises the CJEU's judgment. The UODO points out that data exporters have to make an individual assessment of the level of data protection in the respective third country taking into account not only the contractually agreed upon provisions, but also the legal framework in the third country.

		The UODO emphasises that national supervisory authorities cooperating in the EDPB should act jointly now. It further refers to the EDPB's statement.
RO	**Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal** Link [en]	The Romanian National Supervisory Authority for Personal Data Processing summarises the CJEU's judgment and points out that – in absence of an adequacy decision – data transfers to the US remain possible based on appropriate safeguards in the meaning of Art. 46 GDPR. For further information, it refers to the EDPB's statement and FAQ.
SE	**Datainspektionen** Link [sv]	The Swedish Data Protection Authority informs briefly about the CJEU's judgment and the EDPB's statement.
SI	**Informacijski pooblaščenec** Link [sl]	The Slovenian Information Commissioner summarises the CJEU's judgment and advises companies transferring personal data to third countries to switch to other data transfer mechanisms (eg SCC, BCR) "as soon as possible", provided that data controllers take appropriate safeguards to ensure the protection of privacy. The Slovenian Information Commissioner does not specify the formulation of such appropriate safeguards.
SK	**Úrad na ochranu osobných údajov** Link [sk]	The Slovakian Authority only briefly informs about the CJEU's judgment and refers to the EDPB's statement.
UK	**Information Commissioner's Office (ICO)** Link [en]	In its updated statement, the ICO acknowledges that the CJEU's judgment had wider implications than just the invalidation of the EU-US Privacy Shield. The CJEU's judgment confirmed that the EU standards of data protection must travel with the personal data when it goes overseas. The ICO refers to the EDPB's FAQ and announces that further work by the European Commission and the EDPB is underway to provide more comprehensive guidance. In the meantime, the ICO recommended that "UK businesses should take stock of their international data transfers and react promptly as guidance and advice becomes available". The ICO acknowledged the EDPB's recommendation requiring conducting a risk assessment as to whether SCC provide enough protection within the local legal framework, whether the data transfer is to the US or elsewhere. Finally, the ICO is considering what the CJEU's judgment means in practice. It stated that it would continue to apply a risk-based and proportionate approach in accordance with its Regulatory Action Policy.
US	**US Department of Commerce** Link [en]	In its press release, the US Department of Commerce expresses its deep disappointment and states that it is studying the CJEU's judgment to fully understand its practical impact.

		US Secretary of Commerce Wilbur Ross wants to remain in close contact with the European Commission and the EDPB in order to limit negative consequences to the $7.1 trillion transatlantic economic relationship. It is critical for companies recovering from consequences of the COVID-19 pandemic to be able to transfer personal data without interruption. He also mentions that US national security data access law and practices meet – and in most cases exceed – the rules governing such access in foreign jurisdictions, including the EU. Finally, he states that the US Department of Commerce continues to administer the EU-US Privacy Shield and reminds participating organisations that the CJEU's judgment does not relieve them from their obligations under the EU-US Privacy Shield.
US	**US Department of State** Link [en]	The US Department of State expressed its disappointment with the CJEU's judgment and is reviewing it and its implications. It also stated that the US would "continue to work closely with the EU in order to find a mechanism to enable the essential unimpeded commercial transfer of personal data from the EU to the US".
US	**US Senate Committee** Link [en]	The chairman of the Senate Committee on Commerce, Science and Transportation, Roger Wicker, and the chairman of the Subcommittee on Manufacturing, Trade and Consumer Protection, Jerry Moran, stated that the economic effect of the CJEU's judgment was "troubling". They also stated that invalidating the EU-US Privacy Shield would cause significant disruptions to data transfers and trade activity. They stressed the need to work quickly in order to establish a successor framework that supports economic development and adequately protects consumer data across borders.