EU DATA EXPORT

SHOULD I JOIN THE PRIVACY SHIELD?

The European Court of Justice's ruling in the *Schrems* case, which invalidated the EU-US Safe Harbor framework, has created uncertainty as to how organisations should comply with the EU data export rules for EU-US data transfers. This guidance note outlines the requirements of the new EU-US Privacy Shield framework, which has been designed to replace the Safe Harbor framework.

Background

Under existing EU data protection law and the new European General Data Protection Regulation (the "**GDPR**"), which comes into effect on 25 May 2018, the transfer of personal data outside of the EU is prohibited **unless**:

- the data is transferred to a "White List Country" which ensures adequate protection for that data, based on an EU Commission (the "**Commission**") finding of adequacy;
- the data is transferred to a US entity which self-certifies under the **Privacy Shield**;
- other **Commission-approved adequate safeguards** are put in place to protect that data; or
- a **specific derogation** applies.

White List Countries

Personal data can be freely exported to countries which have been approved as providing adequate protection by the Commission without any further safeguards being necessary.

The Commission maintains a list of its adequacy decisions from time to time (known as the "**White List**") here – as at November 2016 this list includes Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. The White List is expected to be reviewed as part of the implementation of the GDPR to ensure these countries provide a similar level of protection to the GDPR.

EU-US Privacy Shield

On 12 July 2016, the Commission adopted a new US – EU adequacy decision for the **Privacy Shield** framework, which imposes stronger obligations than Safe Harbor on entities in the US who self-certify compliance with its principles. The Privacy Shield became operational in August 2016. This enables an EU entity to transfer data covered by a US entity's certification to that US entity.

Other Adequate Safeguards

The Commission allows entities to put in place "adequate safeguards" to protect personal data, including the use of the Commission-approved **Model Clauses** or the use of Binding Corporate Rules ("**BCRs**") approved by EU regulators to govern transfers between companies.

Model Clauses

There are three sets of Model Clauses, two sets that cover "controller to controller" transfers (where both the importing and exporting party can use the data freely for their own purposes) and one set that covers "controller to processor" transfers (e.g., where the importing entity is a mere service provider and can only process the data in accordance with the instructions of the exporting data controller).

These should be executed in the form approved by the Commission and it falls upon the signing entities to ensure that they are in compliance with their terms. Best practice is to conduct an audit of your organisation's ability to comply pre-signing and then incorporate ongoing compliance with the terms into your central privacy compliance programme, including audits.

EU DATA EXPORT continued

SHOULD I JOIN THE PRIVACY SHIELD?

EU controller to Non-EU/EEA controller

- Decision 2001/497/EC ("**Set I**")
- Decision 2004/915/EC ("**Set II**")

Set I and Set II provide similar levels of protection, but Set II are generally seen as being more business-friendly with respect to liability, litigation, allocation of responsibilities and auditing requirements so tend to be used more frequently.

EU controller to Non-EU/EEA processor

- Decision 2010/87/EU

At this time there are no "processor to processor" Model Clauses, so for data transfers from an EU processor to a Non-EU/EEA processor, another export method must be used or the EU controller must enter into the "controller to processor" Model Clauses directly with the non-EU service provider or grant the EU processor a mandate to enter into the Model Clauses on the data controller's behalf.

In some countries prior approval is needed from the DPA, or the Model Clauses must be filed with the DPA. These requirements will be abolished when the GDPR comes into force.

BCRs

BCRs are internal group rules which amount to a compulsory code of practice governing the processing and transfer of personal data between group entities. They can be used by multinational groups as once approved, they ensure that data from EU-based controllers will be subject to the same level of protection no matter where in the group the data is processed.

To put in place BCRs, you must conduct a detailed review of your operations and then put in place comprehensive rules which are enforceable by data subjects and binding on each member of your group. The BCRs must set out clearly the scope of data, transfers, territories and entities covered, and include provision for: third party beneficiary rights for data subjects, payment of compensation and remediation of breaches of the BCRs, training, audits, complaints handling processes, an internal network of privacy officers or appropriate staff to oversee compliance internally, a description of internal transfers, an update process and group privacy principles.

The BCRs must be approved by the DPA in one EU country (usually the one where you have your main EU operations). Once you submit your BCRs, it will take between six months to two years to obtain approval from the DPAs under the EU recognition procedure, during which time you will need to have alternative safeguards in place. Given the time and cost involved in approval, BCRs are not suitable for all organisations.

Consent and other Specific Derogations

The Commission also permits you to transfer personal data if the data subject **consents** to the transfer of data outside of the EU/EEA or where the transfer is necessary for the performance of a contract at the data subject's consent (e.g., where the goods or services are provided by a non-US provider).

Obtaining consent under the GDPR is not easy - consent generally must be a **freely given**, **specific**, **informed**, **unambiguous** indication of the data subject's wishes, notified by means of a **clear affirmative action** and may be **withdrawn at any time (meaning the data can no longer be transferred)**. Additionally, in the context of data export, the data subject must have been informed of the possible risks of such transfer.

The bar for obtaining valid consent has been raised from the existing EU data protection regime, e.g., under the GDPR consent is unlikely to be considered "freely given" if, for example, the data subject's receipt of your services is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (e.g., use of overseas service providers for storage of data when the service is provided from the UK).

EU DATA EXPORT continued

SHOULD I JOIN THE PRIVACY SHIELD?

Privacy Shield

US entities can register as Privacy Shield companies if they self-certify that they comply with a set of seven key and 16 supplemental "Privacy Shield Principles". Following successful registration, EU entities can transfer the types of personal data covered by the registration to the US registered entity in compliance with EU laws.

The seven key **Privacy Shield Principles** are:

- **Notice** – see "Privacy Shield Notice Requirements" below for more details;
- **Choice** – you must provide clear, conspicuous and readily available mechanisms whereby individuals can opt out of any disclosure of personal data to a third party or the use of personal data for a purpose other than that for which it was collected. For sensitive information, the individual must affirmatively opt in to allow the disclosure of such information to a third party or for use for a purpose other than that for which it was collected;
- **Accountability for Onward Transfer** – you must specify in third party contracts that transferred data may only be processed for limited and specified purposes consistent with the data subject's consent, and you must require third parties to provide the same level of protection as is set out in the Privacy Shield Principles;
- **Security** – you must take reasonable and appropriate measures to protect data from loss, misuse, unauthorised access, disclosure, alteration and destruction;
- **Data integrity and Purpose Limitation** – you must ensure that the data you transfer is limited to that which is relevant to the purposes of the processing and that it is accurate, complete and up-to-date;
- **Access** – you must provide individuals with access to their personal data and with the opportunity to correct, amend and delete information that is inaccurate or processed in violation of the Privacy Shield Principles; and
- **Recourse, Enforcement and Liability** – you must put in place processes for complaints handling and you will be subject to enforcement by the FTC. For more information – see "Focus on Recourse & Enforcement" below.

How to join the Privacy Shield

The first step to joining the Privacy Shield is to **identify whether you are eligible**, as only organisations in the US that are subject to the jurisdiction of the Federal Trade Commission ("**FTC**") or the Department of Transportation ("**DOT**") may participate in the Privacy Shield.

Once you are confident that you are eligible, you need to **audit your organisation** to confirm whether you already comply with the Privacy Shield Principles and identify any gaps where you need to take steps to achieve compliance.

Once you have conducted that audit, you need to:

- **Develop a Privacy Shield-compliant privacy policy statement** before submitting your self-certification to the Department of Commerce ("**DOC**") (see "Privacy Shield Notice Requirements" below).
- **Identify your organisation's independent recourse mechanism:** you must provide an independent recourse mechanism available to investigate unresolved complaints at no cost to the individual.
- **Ensure that your organisation's compliance verification mechanism is in place:** to meet this requirement, you may either use self-assessment or an outside/third-party assessment program.
- **Designate a Privacy Shield contact:** you need to provide a contact to handle questions, complaints, access requests, and any other issues arising under the Privacy Shield. They can be either the corporate officer certifying your compliance with the Privacy Shield framework, or another official within your organisation, such as your Chief Privacy Officer.
- **Review the information required to self-certify:** Prior to submitting a self-certification, your organisation should review and compile the information required as part of the DOC's online self-certification process.
- **Submit your organisation's self-certification to the DOC**: you need to click on the "Self-Certify" link on the Privacy Shield website to create a profile and submit your organisation's self-certification.

EU DATA EXPORT continued

SHOULD I JOIN THE PRIVACY SHIELD?

In addition, once you have fulfilled all of these steps, you will need to pay the annual **fee** to get certified and remain certified under the Privacy Shield. This fee depends on the annual revenue of your organisation and varies from US $250 to US $3,250.

Note that in some EU countries, prior approval is still needed, or a filing will need to be made, even where an organisation is relying on the Privacy Shield to transfer data. These requirements should be abolished under the GDPR.

Privacy Shield Notice Requirements

To comply with the Privacy Shield Notice Principle, your privacy policy must include information about:

- your **participation in the Privacy Shield** (with a link or web address to the online Privacy Shield List) and, where applicable, the entities or subsidiaries of your organisation also adhering to the Principles;
- the **types of personal data you collect** and the **purposes** for which you collect and use such data;
- your **commitment** to applying the Privacy Shield Principles to all personal data you receive from the EU under the Privacy Shield;
- the **rights of individuals to access their personal data;**
- how data subjects can **contact your organisation** with any inquiries or complaints, including the contact details of any relevant establishment in the EU that can respond to such inquiries or complaints**;**
- the type or identity of **third parties** to which you disclose personal information, and the purposes for which you make such disclosures;
- the means your organisation offers individuals to **limit the use and disclosure** of their personal data;
- the individual's right, under certain conditions, to invoke **binding arbitration**;
- the availability of an independent **dispute resolution body** to address complaints and provide appropriate recourse free of charge, including whether such body is: (1) the panel established by DPAs; (2) an alternative dispute resolution provider based in the EU; or (3) an alternative dispute resolution provider based in the United States;
- the **investigatory and enforcement powers** of the FTC or DOT or any other US authorised statutory body, and your company's obligation to disclose personal information in response to **lawful requests** by public authorities, including to meet national security or law enforcement requirements; and
- your **liability** in cases of onward transfers to third parties.

Monitoring & Enforcement

The DOC monitors how organisations comply with the commitments they make as part of the Privacy Shield and identifies organisations which are self-certifying but not compliant, either once their entry on the online Privacy Shield list expires or if they were never compliant but still self-certified. If an organisation **persistently** fails to comply with the Privacy Shield Principles, the DOC may **remove its registration** from the Privacy Shield list and the organisation will have to **return or delete all personal data** received under the protection of the Privacy Shield, as well as being exposed to potential liability under the **False Statements Act** (18 USC. §1001) which may amount to a fine of up to US$500,000 or imprisonment of up to five years, or both. A "persistent" failure will have occurred if an organisation fails to comply with a final determination by any government body or privacy self-regulatory organisation or independent dispute resolution body, or if such body determines that an organisation's failure to comply is significant enough that its claim to comply with the Privacy Shield Principles is no longer credible.

The FTC enforces the Privacy Shield and will review referrals from EU Member States, the DOC or privacy self-regulatory organisations and independent dispute resolution bodies on a priority basis, to determine if, for example, §5 of the FTC Act prohibiting unfair or deceptive acts and practices has been violated e.g., because an entity is not abiding by the requirements of its Privacy Shield compliant privacy policy. If the FTC determines that a violation has taken place, it may seek an **administrative cease and desist order** prohibiting the relevant practice or may file a complaint in a federal

EU DATA EXPORT continued

SHOULD I JOIN THE PRIVACY SHIELD?

district court, which (if successful) could result in a **federal court order** to the same effect. If an organisation then does not comply with the terms of such cease and desist order, the FTC may then bring **civil penalties** (**including fines** of up to US $16,000 per violation or US $16,000 per day for continuing violations which, in the case of practices affecting many consumers, can amount to millions of dollars (for example, in 2012 a well-known ISP paid US$22.5 million to resolve allegations of violation of an FTC order)) against it and if it does not comply with the terms of a federal court order, the FTC may pursue **civil or criminal contempt** for such violation.

Data Export – Ongoing Uncertainty

While the Privacy Shield comes as a relief to companies who previously transferred data to the US under the Safe Harbor framework, the framework has faced some heavy criticism from privacy activists, the Article 29 Working Party and the EU Commission who claim that it does not go far enough. Further, as Facebook's use of the Model Clauses has also been challenged in the Irish courts, in a case where the substantive issues have now been referred to the European Court of Justice, it seems likely that the Model Clauses also face challenge as an inadequate means of securing the protection of transferred personal data – although we will not know the outcome for some time. Given the limitations of BCRs in terms of time and cost, and the difficulty of obtaining valid consent under the GDPR, it appears that for now, the Privacy Shield and the Model Clauses remain the most flexible approaches to transferring data outside of the EU at the current time, despite some risk of future challenge.

We have evaluated the most relevant export mechanisms for global data export on the following page.

APPENDIX 1

DATA EXPORT MECHANISMS COMPARED

	White List Countries	Privacy Shield	Model Clauses	BCRs	Consent
Description	Transfer to country which is the subject of an adequacy decision (see below).	Compliance with the Privacy Shield Principles (see above) and self-certification.	Execution of un-amended Commission approved Model Clauses for "controller to controller" or "controller to processor" (not "processor to processor").	Intra-group rules on data transfer and processing to be put in place and authorised by EU DPAs.	Consent must be freely given in accordance with the requirements of the GDPR.
Territories	As of 1 November 2016, Andorra, Argentina, Canada[1], Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay.	United States (only Privacy Shield-certified companies).	Global ex EU.	Global ex EU for intra-group transfers only. Not recognised by all EU DPAs until the GDPR comes into effect.	Global ex EU.
Onward Transfers	Onward transfers subject to the laws of the relevant White List Country.	Onward transfers subject to the Privacy Shield onward transfer rules, which require onward recipients to comply with the Privacy Shield Principles.	Onward transfers subject to the requirements of the Model Clauses, which require onward recipients to be subject to Model Clauses or otherwise comply with EU law.	Onward transfers subject to the requirements set out in the entity's BCRs, which would typically require compliance with the requirements of EU privacy law.	Onward transfers must be covered by the scope of the original consent.
Time	Fast (export is automatically permitted).	Moderate (assuming entity is already Safe Harbor-compliant, the additional steps to achieve compliance with the Privacy Shield Principles and self-certify should take up to six months, depending on the organisation).	Fast (assuming entity is already compliant with the requirements of EU privacy law). Although note additional time may be needed to ensure compliance with the terms of the Model Clauses.	Slow (assuming the entity is already compliant with the requirements of EU privacy law, it will still take six months to two years for the EU approval process to be completed).	Fast – if consents in place. Moderate to slow if consents need to be sought.
Ease	Easy (export is automatically permitted without additional safeguards).	Moderate (assuming entity is already Safe Harbor-compliant – self certification is	Easy/moderate depending on the number of entities.	Hard (assuming the entity is already compliant with the requirements of	Moderate (there is a high bar for establishing valid consent and consent

[1] *Companies subject to SIPCDA*

APPENDIX 1 continued

DATA EXPORT MECHANISMS COMPARED

	White List Countries	Privacy Shield	Model Clauses	BCRs	Consent
		fairly straight-forward but steps may be required to achieve full compliance with the Privacy Shield Principles).		EU privacy law, BCRs still need to be documented and the EU approval process facilitated, including responses to enquiries, etc.)	may be withdrawn at any time).
Internal Costs	N/A	Moderate upfront and low ongoing costs (assuming entity is already Safe Harbor - compliant – steps may be required to achieve full compliance with the Privacy Shield Principles, including a full audit and costs of advisers).	Low upfront and ongoing costs (assuming entity is already compliant with the requirements of EU privacy law and the specific requirements of the Model Clauses).	High upfront costs and low ongoing costs (even assuming the entity is already compliant with the requirements of EU privacy law, typically a full audit is required and external advice to put in place the BCRs and to facilitate the EU approval process, including responses to enquiries, etc.)	Moderate - there may be significant costs involved with seeking consent depending on your business model.
Fees	N/A	Low – annual fee of US $250 to US $3,250 depending on size of the organisation.	N/A	N/A	N/A
Liability	Potential liability to EU DPAs, via criminal or civil sanctions (currently up to £500,000 in the UK), which will increase on 25 May 2018 to up to EUR 20 million or 4% of global turnover.	Potential liability to FTC and DOC (see above) e.g., where the US entity fails to comply with an FTC administrative order, the FTC may impose a fine of up to US $16,000 per violation or US $16,000 per day for continuing violations which may amount to millions of dollars.	Potential liability to EU DPAs, via criminal or civil sanctions (currently up to £500,000 in the UK), which will increase on 25 May 2018 to up to EUR 20 million or 4% of global turnover.	Potential liability to EU DPAs, via criminal or civil sanctions (currently up to £500,000 in the UK), which will increase on 25 May 2018 to up to EUR 20 million or 4% of global turnover.	Potential liability to EU DPAs, via criminal or civil sanctions (currently up to £500,000 in the UK), which will increase on 25 May 2018 to up to EUR 20 million or 4% of global turnover.