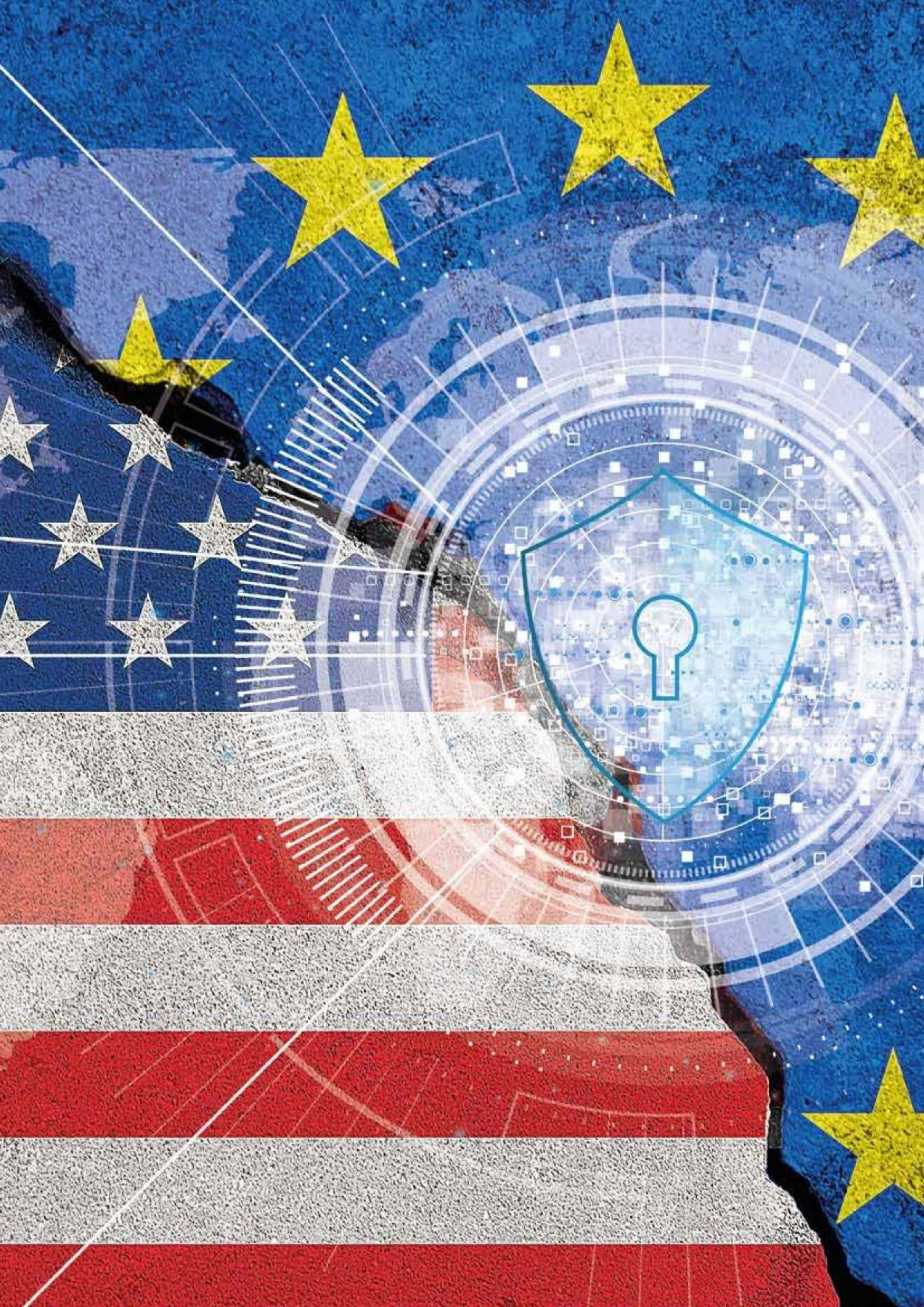




Barry McManus

EUROPEAN COURT OF JUSTICE RULES AGAINST EU-US PRIVACY SHIELD



The European Court of Justice (ECJ) ruled on the 16th of July 2020 that the EU-US Privacy Shield did not afford enough protection against surveillance practices by US intelligence agencies^{1,2} on Personal Identifiable Information (PII) transferred from Europe to the US, as per Article 45 of GDPR (Article 45 is concerned with a third country providing adequate level of protection³). To recap, GDPR is concerned with the secure processing of PII outside of the EU.

There are four avenues for this to occur³:

- 1) **Third country adequacy:** PII can be processed within countries that are recognised by the EU to have an adequate level of data protection, such as New Zealand, Switzerland and Uruguay⁴.
- 2) **Specific treaty:** for the US, secure processing of PII could not be ascertained and the EU-US Privacy Shield Treaty was established to ensure data privacy and security. This treaty was the focus of the ECJ ruling.
- 3) **Individual contract:** a business transferring PII puts in place certain safeguards to ensure protection via a contract, such as: the subject matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into consideration the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. This may be an individual contract or Standard Contractual Clauses (SCCs)^{5,6} which are adopted by the commission or by a supervisory authority.
- 4) **Inter-organisation transfer:** Binding Corporate Rules (BCRs), similar to contracts, are corporate policies enforced by every sub member of a multi country organisation.

‘To recap, GDPR is concerned with the secure processing of PII outside of the EU.’

DEFINITIONS

PERSONAL IDENTIFIABLE INFORMATION/PERSONAL DATA

Information relating to an identified or identifiable natural person, such as name, location data or online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity³.

CONTROLLER

Determines the purposes and means of the processing of personal data³.

PROCESSOR

Processes personal data on behalf of the controller³.

SUPERVISORY AUTHORITY

Independent public authority which is established by a Member State³.

BINDING CORPORATE RULES

Personal data protection policies which are adhered to by a controller/processor established ‘in’ a Member State for transfers... of personal data to a controller/processor in one or more third countries within a group of undertaking³.

RULING

The ECJ stated that the SCCs (and BCRs) are valid for the transfer of data between EEA and non-EEA countries. However, it is under the remit of controllers/processors to determine whether the laws of the destination country are contrary to the requirements of the SCC and additional safeguards may need to be defined. Under SCC, the obligation to ensure data protection is the responsibility of the data controllers⁷. If a controller feels that data transfer to a third country, (including any additional safeguards) fails to provide protection, the data transfer should cease. Should the controller fail in this regard, the onus is on the supervisory authority to do so⁷.

HAS ANYTHING REALLY CHANGED?

As a result, due diligence of SCCs is required and it appears that the ECJ is reinforcing requirements listed within GDPR³:

- Paragraph 81 indicates that ‘the activities performed by the processor should be governed by a contract’
- Paragraph 28.7 indicates that the Commission may lay down Standard Contractual Clauses for the items listed in Article 28.3 and Article 28.4
- Paragraph 28.3 states the processor:
 - (a) Processes on the documented instructions of the controller

- (b) Is committed to confidentiality
 - (c) Takes all measures detailed in Article 32 (security of processing, based on risk: data pseudonymisation and encryption; ensure confidentiality, integrity, availability and resilience of processing; restore access to data; regular assessment of technical and organisational measures for security of processing)
 - (d) Ensures due consideration for engaging another processor
 - (e) Ensures data subject rights (right to be forgotten, correction, deletion, etc.)
 - (f) Notifies of data breach and data impact assessment (in the event of high risk to the data subject)
 - (g) Deletes or returns personal data at the end of processing
 - (h) Provides information to demonstrate compliance
- Paragraph 28.4 states that the same obligations shall be imposed on a sub processor when a processor engages a sub processor via a contract.

Given that the US-Privacy Shield was a self-certifying process, then it should not have been used to provide the sole level of comfort when considering US located PII processing and storage. Due diligence of contracts was always required.

EXAMPLE OVERSIGHT ACTIVITIES

Some examples of SCC due diligence activities for data controllers to consider may include (in no particular order):

Data Analysis

- Identify the PII processed by the processor (for example, if special category data)
- Determine the scale of processing (for example, is the data adequate, relevant and limited to what is necessary in terms of processing?)
- Confirm the lawfulness of processing of PII (for example, consent, contract performance, compliance to legal obligation, legitimate interests of processor)
- Determine the location of processing of data and data storage and the level of protection afforded. Establish if PII data processing is performed only for the purpose it was collected. Establish the scope of any sub processor involvement and apply the same approach to them
- Assess the impact that the processing operations may have on the protection of PII.

Operational Analysis

- Assessment of technical and procedural measures, for example:
 - Perform non-functional testing (security) of the system within a dedicated test environment to verify, for example, encryption in transit and at rest or system resilience and recovery (security of processing)
 - Monitoring of architecture, including logs, static analysis tools
 - Qualification of key processes and security controls.
- Verification of procedures to exercise data subject's rights, such as data correction requests, incidence response (data breach and remediation) and complaints procedure.

'In the interim, many US-based processors will be seeking to implement SCCs in order to ensure compliance to GDPR.'

Review

- (Where feasible) audit/inspect the processor's technical and operational controls including design, building in protection and operational controls (especially the infrastructure)
- Review artefacts such as licenses, contracts, SOC II report, (GDPR) privacy statements/notices, defined SCCs(8), security statements, disaster recovery and business continuity test activities, public bug bounty programmes, oversight of third party suppliers/sub processors and so forth.

FINAL THOUGHTS

As noted by the Guardian¹ and Wired², the ECJ ruling may also muddy the waters of future EU-UK data transfer discussions during the ongoing Brexit talks, with the UK seeking unrestricted data transfers with the EU and with the US based on a de-facto UK Privacy Shield.

Where the EU, US and the UK go with GDPR is currently undetermined. Given the historical event of EU-US Privacy Shield replacing Safe Harbor, then it can be assumed that another treaty will be discussed.

In the interim, many US-based processors will be seeking to implement SCCs in order to ensure compliance to GDPR. However, the privacy responsibility is also a remit of the data controller who should be satisfied that adequate protection is in place.

REFERENCES

- 1) Tech firms like Facebook must restrict data sent from EU to US, court rules, www.theguardian.com/technology/2020/jul/16/tech-firms-like-facebook-must-restrict-data-sent-from-eu-to-us-court-rules Guardian, 16 July 2020
- 2) The end of Privacy Shield spells trouble for Brexit Britain, <https://www.wired.co.uk/article/privacy-shield-future> Wired 17 July 2020
- 3) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
- 4) European Commission Adequacy Decisions, Recognised countries that offer adequate level of data protection, <https://gdprinformers.com/gdpr-articles/data-transfers-third-countries>
- 5) Example SCC: European Data Protection Board Website, January 2020 https://edpb.europa.eu/sites/edpb/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf
- 6) Source of example SCC: Register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism, European Data Protection Board website <https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions>
- 7) Paragraphs 108 and 134/135, Case C 311/18, JUDGMENT OF THE COURT (Grand Chamber), 16 July 2020, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227>

PROFILE

Barry is a Principal Consultant for Empowerment Quality Engineering Ltd, a Computerised System Validation consultancy that bridges the gap between IT and Quality. Barry focuses on building quality and security into Computerised Systems (CS) by using quality techniques from the wider software industry while ensuring regulatory compliance. He leads GxP CS validation compliance and IT supplier/ service provider audits across the globe, performs IT supplier's software lifecycle process improvement and performs risk assessments to drive validation strategies and tailored training. Barry has over 23 years of experience in software engineering and IT administration with vast technical knowledge of every role and every activity within the CS lifecycle; development methodologies (traditional and agile), databases and programming languages across multiple technologies. He moved into the regulated industry in 2003 to commence management roles in QA, QC and CS validation and his approach resulted in delivering risk-based, on time, right first time CS validation projects. Barry's experiences ensure that technical and regulatory risks do not compromise CS validation projects, delivers 'value add' CS validation documentation and GxP compliance. He is a member of the RQA IT Committee, the DIA IQCT community core team and a member of the ISPE Data Integrity Project Team.

