Legal alert for BCS members & IT professionals on the data protection judgment, known as Schrems 2[1], by the Court of Justice of the European Union.

Prepared by

- Daniel Aldridge, Senior Policy Manager – BCS
- Dott. Chiara Rustici, Chair - BCS Law specialist group
- Dr Sam De Silva, Partner - CMS Cameron McKenna Nabarro Olswang LLP
- Ian Fish, Chair - Information Security specialist group

BCS, The Chartered Institute for IT

With Technology playing such a pivotal role in our daily lives, it's paramount that those working in computing recognise their place in progressing IT for the benefit of society. The purpose of the BCS is to promote and advance the education and practice of computing for the benefit of society. We bring together industry, academics, practitioners, and governments to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and body for IT, we serve over 60,000 members including practitioners, businesses, academics, and students, in the UK and internationally. We also accredit the computing degree courses in ninety-eight universities around the UK and offer a range of widely recognised professional and end-user qualifications.

Introduction

The July 16th 2020 judgment by the Court of Justice of the European Union, known as Schrems 2, has immediate implications for any organisation doing business by transferring personal data to USA based organisations, and for any organisation doing business by transferring personal data to organisations based in countries the EU does not recognise as having an adequate level of protection for data protection[1]. On August 10th, 2020, European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross announced that discussions to evaluate the potential for an enhanced EU-U.S. Privacy Shield framework to comply with the CJEU's Schrems 2 have started[2].

Our understanding of the implications of the Schrems 2 judgment is still evolving: this paper only suggests immediate practical actions and initial policy thoughts. Furthermore, it is a call to action for the UK's IT professional and business communities to pay due care and attention to Schrems 2 to safeguard their businesses and operations as much as possible. Other policy actions and briefing papers are currently being considered by BCS as more evidence is collected from members and more guidance is offered by data protection authorities. This paper is not intended to constitute legal advice. Specific legal advice should be sought before taking or refraining from taking any action in relation to the matters mentioned in this paper.

Scope of Schrems 2

- All organisations are affected, from multinational to not-for-profit, to the extent that their data and information flows include personal data
- Organisations based in the EU and USA are not the only ones in scope: any organisation may be relying, directly or indirectly, in some part of their value chain, on personal data flows affected by this judgment
- Personal data is defined under the GDPR broadly to include data with the potential to identify living individuals, whether structured or unstructured, audio-visual, or biometric, whether it is already in the public domain or not.
- All forms of personal data/information flows of personal data are affected, as the legal definition of "data transfer" encompasses streaming, over the top telecommunication data, access from one country to databases physically located in another, as well as data storage mediums physically transferred from one country to another
- While the ramifications are still being analysed by the privacy community, as of July 16th, technically, organisations that do not comply with that Court's judgment face potential

[1] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[2] https://www.huntonprivacyblog.com/2020/08/10/european-commission-and-u-s-department-of-commerce-to-discuss-enhanced-eu-u-s-privacy-shield-framework/

legal liability and fines up to 4% of global turnover. No grace period has been allowed by the European Data Protection Board.

- From a practical perspective, no one should attempt to second guess whether data protection authorities will immediately launch investigations or impose fines against the companies that have relied on Privacy Shield or not. However, affected organisations should have a plan for how they are going to address the issues, start implementing that plan as soon as reasonably practicable, and be ready to discuss with relevant stakeholders as needed.

Ten immediate actions:

1. Assess how much of the personal data your organisation handles are strictly mission-critical and how much is expendable. Minimize your organisation's personal data. Be mindful that most business data are also personal data and that most datasets are mixed, and it may be impossible to segregate personal from non-personal data.

2. Assess in which countries your personal data ends up routinely or occasionally, directly, or indirectly, via cloud services, web-based applications, cookies and other trackers, contractors, sub-contractors and suppliers. Map all the organisation's personal data flows you are responsible for against the interactive data protection map produced by CNIL[3]. Keeping a real-time visual of how your personal data ecosystem crosses national boundaries and of how data protection requirements for data transfers change will be useful also for upcoming changes in countries' data protection status. Consider whether your transfer counterpart is a likely target for government intelligence surveillance demands.

3. Audit who has access rights to your organisation's personal data sets (databases, data streams, data repositories of any kind) and from which countries they can access them. Be mindful that, in legal terms, to access data is to transfer data. Include in this audit of permission levels: clients, business partners, employees, remote workers, freelancers, temps, interns, volunteers.

[3] https://www.cnil.fr/en/data-protection-around-the-world

4. If you have an in-house legal department, they should have reached out to the IT team by now. If you use external legal counsel , they may not have contacted you yet, so be proactive: re-read your own policies and search the terms and conditions of your suppliers, contractors and subcontractors[4] to identify which data flows in your organisation rely, directly or indirectly, on a "Privacy Shield" clause[5]. This is a legal basis for transferring data to the USA that is now invalid. Do the same search for Standard Contractual Clauses (SCC). These are still valid but require additional action on your part. For example, to continue to use SCCs you will need to undertake due diligence to evaluate and document the risks associated with those transfers. In practice, you will need to identify if the laws of the destination country cause concern in relation to the rights of data subjects (see action 2). To identify potential risks, an assessment of the third country's laws and potential international commitments is now necessary and recommended by the European Data Protection Board. You should also ensure the data importer in the destination country understands that it needs to notify you of laws and other obligations that would prevent it from complying with the SCCs, including being subject to any specific government surveillance or legal monitoring.

5. Address highest risk transfers first. For example, a financial institution is likely to have high levels of risk, whereas a small online retailer is likely to have lower levels of risk of surveillance interception. Where it is possible that US governmental authorities might seek to access the personal data transferred, consider including additional protections, such as encryption or tokenization, which could render personal data meaningless to a third party, or adding suspension or termination clauses in contracts that allow the data exporter to minimise the risk of an enforcement action in the EEA and the threat of fines.

6. Once you have quantified the amount and kinds of personal data transfers to the USA, servers controlled by US companies or other countries outside the European Economic Area (EEA) which do not provide adequate safeguards, escalate the matter to the highest level of risk ownership in your organisation.

7. Be in the room when management works out the cost-benefit analysis of practical solutions for the parts of your business that rely directly or indirectly on Privacy Shield or SCCs. There may be several solutions. None is without consequences. Go to the meeting prepared to offer key figures of data transfers, and your assessment of IT architecture workarounds.

[4] https://www.privacyshield.gov/list
[5] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

8. IT additional safeguards or alternative IT architecture workarounds may not be the only solutions to Privacy Shield-based data transfer to the USA or data transfers based on SCCs to those countries which do not provide adequate safeguards:

    a) Business alternatives include redesigning which type of business processes are carried out by which country's business unit or switching to cloud and other IT suppliers which are not subject to the jurisdiction of the US or of other countries which do not provide adequate safeguards.
    b) Legal alternatives include replacing Privacy Shield with SCC with "additional safeguards" as the legal basis for transfers or relying on one of or more of the specified "derogations[6]" in Article 49 of the GDPR or, in the case of multi-national organisations, considering the use of Binding Corporate Rules (BCRs).
    c) IT alternatives include re-allocating personal data access privileges to staff in the EEA, arranging for the business' personal data to be processed exclusively by staff based in the EEA, adding encryption layers and ensuring encryption keys are in your possession, or anonymising personal data.

9. Continue to monitor developments. The interpretation and application of Schrems 2 is rapidly changing and developing. We are expecting more guidance from authorities and other developments very soon. IT professionals should stay closely aligned with these developments and adjust their plans accordingly.

10. Work with your colleagues and professional communities to influence positive change. Organisations like the BCS depend on the collective skills and knowledge of our volunteer member communities working across many disciplines to advance the cause of computing and technology for good. More information about becoming a BCS member can be found here: https://www.bcs.org/membership/become-a-member/.

[6] https://gdpr-info.eu/chapter-5/