Adequacy Decision on EU-US Data Protection to Enable Transfers of Personal Data

July 10, 2023, the European Commission adopted a new adequacy decision for safe and trusted EU-US data flows, based on the EU-US Data Privacy Framework (DPF). The US have established effectively the same frameworks with the UK and Switzerland, which will enable data transfers from when the respective UK and Switzerland adequacy decisions will soon be effective. A Swiss adequacy decision for the US may be expected any time after Sept 1, 2023, when the Swiss Federal Data Protection Act will enter into force.

After the EU-US Privacy Shield was invalidated by CJEU (Schrems II) in 2020, The DPF builds on the instruments which were included in the US Privacy Shield and were not per se criticised in the judgement (but require a case-by-case "transfer impact assessment") and aims to remediate the reasons for the invalidation of the Privacy Shield, notably the potential unproportional access to personal data by US authorities and the lack of independent remediation route for individuals.

To that end, the US President has issued an Executive Order which requires US intelligence to implement additional procedures. Under this order, US intelligence services can continue to collect personal data on anyone, anywhere for any purpose typically serving the national security of the US or its partners and allies, with the aim to achieve a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties for all persons. Bulk data collection remains possible if targeted collection is not reasonably and technically feasible, albeit it should be minimized to not disproportionately impact privacy and civil rights and should take into account possible safeguards, e.g. the nature and extent how such information is shared with foreign governments and organisations. A newly created Civil Liberties Protection Officer will review qualifying complaints (submitted via the respective foreign authority from Qualifying States, the individual has no standing in the court) and bring it to a "Data Protection Review Court" (part of the executive administration), who's concluding disclosure will be limited to whether or not a remediation action was decided. The list of Qualifying States is determined by the Attorney General of the US Justice Department based on US national interests (currently EU and its Member States, Iceland, Norway and Liechtenstein, expected to be expanded to Switzerland and UK as and when their adequacy decisions become effective).

Key Elements of the EU-US Data Privacy Framework (DPF)

US businesses and organisations regulated by the Federal Trade Commission or US Department of Transport Services (can be extended to other sectors) can register and self-certify and submit themselves to the principles of the DPF to which they then have to comply.

Protection is limited by court order, law enforcement or security or public interests, statute, or regulatory authorisations to the extent those require. Exceptions and derogations in GDPR are also allowed under DPF, if applied in comparable context. Participating organisations are expected to apply the higher protection of the DPF and US law where possible.

The basic definitions in DPF and GDPR are equivalent. Organisations participating in DPF declare to **notify** individuals and allow them **choice** (opt out) of processing or disclosure to 3rd parties and **opt-in**

for sensitive personal data, however a company does not have to offer the choice (consent) upon subcontracting to other organisations as agents of themselves. Appropriate measures of **security** must be taken, and **purpose and retention limitation** apply. **Individuals have access** to their information and the right to correct or delete it, if incorrect or processed in violation with the DPF, **unless the burden or cost of providing access is disproportionate** to the risks to the individual. A readily available **independent mechanism of recourse** must be made available at no cost to the individual. The participating **organisation remains liable for compliance** also when it passes on processing to an agent, unless it proves that it is not responsible for the event which gave rise to the damage.

Supplementary principles: **In some cases, opt-in is not required for sensitive data**, e.g. if necessary for medical or diagnosis, or by a foundation or other not-for-profit organisation if processing happens for its members only and is not disclosed to third parties. There are also journalism **exceptions** to balance the constitutional freedom of speech with the personal data protection rights and for mere data transfer by telecom or internet providers, as well for due diligence or audit operations. Participating organisations who commit to cooperate with data protection authorities (DPA) must cooperate and comply to their advice on unresolved complaints. They will **self-certify** and perform **self-assessment or outside compliance reviews** to verify. Organisations can opt to handle also human-resource related personal data according to DPF (respecting the law applicable in the state where it was collected and cooperating with EU authorities and meeting EU employer obligations). Commercial secrets can be protected and **access to data handled solely for research or statistical purposes may be denied**. Data transfers to the US and for transfers to third parties (but not necessarily within a controlled group of organisations) require a contract. A **recourse mechanism** in participating organisations can be implemented in a private compliance program, via a supervisory authority or through cooperation with data protection authorities. **Individuals have an arbitration option** for fully or partly unremedied complaints. Sanctions must be effective to correct non-compliance and ensure compliance. Organisations can be **removed from the DPF list for persistent non-compliance**.

Specific Points for the Health Sector Companies

For pharmaceutical and medical products **EU/member state law applies to data collection and DPF applies once the data is transferred to the US**. Such data should be anonymized where appropriate. Where data collected is transferred to the US under the DPF, it **may be used for new studies if appropriate notice and choice was given** in the first instance. It is understood that not all future uses can be specified, and re-use is permitted if consistent with the purpose of the original collection. Where appropriate, the **notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated**. Similarly clinical trial data collected prior to withdrawal from the study may still be processed (up to that point). **Transfers to authorities for regulatory and supervisory purposes are allowed** (also for efficacy and safety monitoring) and access need not be granted to individuals for blinded studies. They should primarily address their physician or health care provider for such inquiries. Key coded (pseudonymized) data qualifies as personal data under the DPF.

Some of these aspects are not firmly established in the EU (ambiguity in GDPR interpretation) and therefore may be challenged or indeed so clarified in court if they are addressed to the court.

Schrems III - or will the Adequacy Decision hold in Court?

The EU-US Adequacy decision will be challenged in court, on the perception of marginal improvements to redress the Privacy Shield but not fundamentally giving non-US persons personal data protection equivalent to GDPR and standing in front of an independent US court and bulk data collection still possible where target data collection is not reasonably and technically possible.

There is a considerable risk that the CJEU may also invalidate the adequacy of the EU-US DPF, triggering repeated disruptions, so depending on what questions are referred to the Court, notably for reasons that both the EDPB and the EU parliament have voiced (bulk data collection, equivalent standing of individuals in US court and law, limitations and differences in proportionality)

Our Viewpoint

Until an adequacy decision is invalidated by the competent court, it holds and hence will provide eligible organisations a convenient mean to interoperate across borders and exchange personal data as needed. Given the uncertainty of such potential judicial verdict, companies may still want to establish laborious transfer impact assessments on Standard Contractual Clauses with their collaborating parties. A potential future CJEU invalidation of the EU-US DPF could also taint the EU-Swiss Adequacy decision or the EU-UK adequacy decisions, once Switzerland and UK are part of the DPF framework too. Transfers via other states with established US DPF adequacy may become an additional fallback option. Given the paramount economic interests involved to exchange personal data smoothly among these countries, they can expect that authorities will likely be supportive within the room they are given.