DORSEY
DORSEY+WHITNEY LLP

A New Scheme is in Place to Allow U.S. Organisations to Import and Use Personal Data from the European Union – Should Every Business Rush to Sign Up?

September 13, 2023 – The TMCA
by Ron Moscona

On 10 July 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework ("DPF"). The adequacy decision is designed to relieve U.S.-based businesses and other institutions and organisations that choose to participate in the DPF from legal uncertainties and administrative burdens in relation to personal data records originating from the EU.

It is expected that the UK and Switzerland will soon adopt similar decisions that will allow participating organisations to enjoy the benefits of the DPF in relation to data imported from those two countries for processing in the U.S. or by U.S. organisations.

The DPF is the third attempt to create a data bridge between the EU – with its heightened concern for protecting privacy interests of individuals – and the U.S., which has been for the past few decades slow in adopting policies and legislation to protect those rights (although more recently consumer privacy legislation is increasingly being adopted by US state legislatures).

Even before the EU introduced its General Data Protection Regulation ("GDPR"), there was a self-certification scheme in place – not altogether unlike the new DPF – which allowed US-based companies and organisations to import personal data from the EU on the basis of the organisation's legal commitment to safeguard the data and to protect the interests of data subjects. Just like the new DPF, under that scheme (the "Safe Harbor" arrangement), mechanisms were put in place to allow the U.S. Department of Commerce to enforce the commitments of participating organisations and to allow individuals to bring complaints. Just like the DPF, the "Safe Harbor" scheme was approved by the EU Commission under applicable EU law.

GDPR was designed to allow the "Safe Harbor" scheme to continue to operate. It contained specific provisions empowering the EU Commission to enter into international

Related People

- Ron Moscona

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

arrangements like the “Safe Harbor” and the DPF. But in its decision of 6 October 2015 in the Maximilian *Schrems v Data Protection Commissioner* case (C-362/14), the EU Court of Justice held that the “Safe Harbor” scheme failed to meet the requirements of EU law in relation to the protection of personal data when it is taken outside the jurisdiction of the EU.

In 2016, the EU Commission approved a second scheme, known as the EU-U.S. Privacy Shield. That scheme was once again ruled in a subsequent decision of the EU court of 16 July 2020 (*Schrems II*, C-311-18) to have fallen short of EU legal requirements.

In both decisions, the main reason for the EU Court’s decision that personal data transferred to the U.S. under the terms of the schemes was not sufficiently protected, was the evidence that U.S. national security and law enforcement agencies were engaged in wide-range, on-going, and (according to the Court’s findings) indiscriminate mass monitoring and surveillance of communications which the agencies access through “back doors” provided by social media and other digital platforms based in the U.S. The rulings of the EU Court were particularly focused on the absence of legal redress mechanisms in the U.S. for EU individuals whose data is or may be exposed to such surveillance.

The EU Commission gave its blessing to the new DPF scheme based largely on the signing by President Biden on 7 October 2022 of Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence laying down limitations and safeguards for all U.S. signals intelligence activities and on a supplemental Regulation on the Data Protection Review Court (28 CFR Part 302) issued by the U.S. Attorney General.

Among other things, the Executive Order and the associated Regulation establish a tribunal and proceedings that affected EU individuals will be able to use to bring complaints regarding the use of their data by intelligence agencies. Those redress mechanisms and the other requirements of the DPF program were considered to be sufficient by the EU Commission to provide adequate safeguards to protect personal data transferred to the U.S. under the scheme.

But what does this all mean for U.S. businesses, organisations, and institutions that consider signing up for the DPF program?

Participation in the scheme means that the organisation will be free to collect, import, and use personal data records from any source in the EU without having to put in place transfer agreements with each data exporter and carry out transfer impact assessment in each case and without risking challenges against its use of personal data imported from the EU. This could be of real benefit for businesses and organisations that receive data regularly from the EU, particularly if they deal with many different categories of personal data, coming from different sources and processed for many different purposes. Self-certification under the DPF means that there is no need to address each and every one of those data transfers individually.

Further, businesses and organisations love to declare that they respect people’s privacy

and that they are committed to protecting personal information. By committing itself to the requirements of the DPF program, an organisation may be able to nurture the trust of other businesses, and organisations, and even the public itself, for being an organisation that truly respect the privacy of individuals and is committed to protecting their data. If the scheme is successful in attracting large portions of corporate America as well as various other organisations and institutions that may be eligible for the scheme, it might become a 'must have' for large companies in the public eye.

The scheme undeniably offers advantage for some, but the administrative effort and the compliance burden in participating in the DPF should not be understated. One of the key criticisms of the defunct "Safe Harbor" scheme was that it lacked any real oversight or enforcement mechanisms. This is not the case with the DPF.

The fundamental idea of the DPF (as any other mechanism to legitimise international data transfers outside the EU) is that the self-certifying organisation has to commit itself to a set of basic "Principles" which reflect the fundamental requirements of the GDPR, including securing for data subjects the same rights that they have under EU law. This in itself is a serious compliance burden which any organisation that contemplates joining the scheme should consider carefully.

Alongside broad principles of establishing a legitimate basis for the use of data, particular protections for sensitive data, data security, controls over the re-purposing of personal data, and the sharing of data with third parties, the DPF also includes some very specific requirements.

These include, among other things, specific information that has to be made available to data subjects regarding the organisation's participation in the DPF scheme, the internal complaints handling procedures, and the external dispute resolution mechanism to which the organisation commits itself and other information. This means that participants would have to update their privacy policies to include this information.

Participating organisations are also required to give data subjects certain specific choices – an opt-out from disclosures to third parties (other than service providers) and an opt-out from re-purposing the data. Apart from the implications of offering those choices, organisations would have to consider the logistics of offering these choices to all EU individuals whose data is being imported by the organisation into the U.S.

Further, the DPF introduces a new set of requirements regarding the contractual arrangements that have to be put in place when the imported data is being shared with a third party controlling (that is, not a service provider which deals with the data on behalf of the participating organisation). Organisations will therefore need to set themselves up for new procedures and new contract forms for dealing with onward transfers.

Another key element – which was lacking in the original "Safe Harbor" scheme but had already been addressed under the "Privacy Shield" program - is the requirement that the participating organisation must submit itself to external dispute resolution mechanisms. Those could take the form of private dispute resolution organisations, but there is also

the option for an organisation to submit itself to the jurisdiction of data protection regulators in the EU. Either way, the requirement is that the mechanism must be free to the complaining individual.

Finally, to ensure that participants maintain the privacy and data security standards to which they commit themselves through self-certification, the scheme requires participating organisations to verify their own compliance. Verification can take the form of self-audits or external audits. Either way, the verification needs to demonstrate that the participant's privacy policy regarding personal information received from the EU is accurate, comprehensive, readily available, conforms to the "Principles", and – importantly – that it is fully complied with. It must also indicate that individuals are informed of the organisation's in-house complaint handling procedures and of the independent recourse mechanism(s) through which individuals may pursue complaints. Further, the verification needs to confirm that the participating organisation has in place procedures for training employees in the implementation of the privacy policy, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above.

An annual self-certification declaration must be made each year confirmed by the declaration of a corporate officer. Executives would need to ensure their companies are indeed fully compliant before swearing such a declaration.

Alongside the compliance burdens and verification and dispute resolution mechanisms, the DPF also includes a number of exceptions and provisions that apply to specific situations, such as allowances for journalism, airlines, and for corporate due diligence exercises, and special rules for clinical trials and medical research and for handling human resources data. These special rules are designed to ensure that the scheme's requirements are not going to be prohibitive in respect of such activities or for organisations in the relevant sectors. They would require particular attention by affected organisations. Consideration of those sets of special rules is beyond the scope of this note.