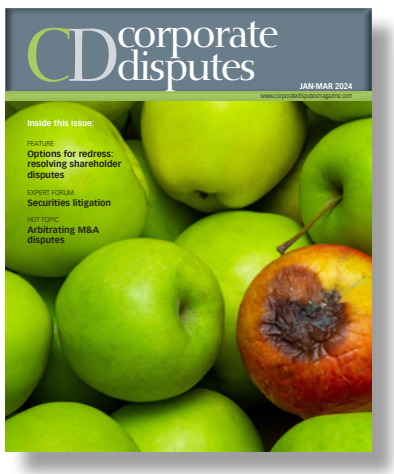
REPRINT

CD corporate disputes

THE NEW DATA PRIVACY FRAMEWORK: PRIVACY SHIELD'S REPLACEMENT

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
JAN-MAR 2024 ISSUE



www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

ICDR INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION® | AMERICAN ARBITRATION ASSOCIATION®

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

PERSPECTIVES

THE NEW DATA PRIVACY FRAMEWORK: PRIVACY SHIELD'S REPLACEMENT

BY **LUIS M. MARTINEZ**
> INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION (ICDR)

The European Union (EU)-US Data Privacy Framework (EU-US DPF), the UK Extension to the EU-US Data Privacy Framework (UK Extension to the EU-US DPF) and the Swiss-US Data Privacy Framework (Swiss-US DPF) were developed to facilitate transatlantic commerce by providing US organisations with reliable mechanisms for personal data transfers to the US from the EU and European Economic Area, the UK (and Gibraltar) and Switzerland consistent with EU, UK and Swiss data protection laws.

The DPF programme was developed in response to the invalidation of the Privacy Shield Framework by the Court of Justice of the European Union (CJEU) in 2020. The CJEU found that the Privacy Shield did not adequately protect EU citizens' personal data from access by US intelligence services.

Why is this important?

US organisations need the DPF programme to comply with EU, UK and Swiss data protection laws, such as the EU General Data Protection Regulation (GDPR), one of the strictest data protection laws in the world. It requires businesses that process the personal data of EU citizens to comply with certain requirements, such as obtaining consent for data processing and providing individuals with access to their data, deleting data when it is no longer

necessary, implementing appropriate technical and organisational measures to protect personal data, and transferring personal data only to countries outside the EU that have adequate safeguards in place.

Fines for violating the GDPR can be significant – up to €20m or 4 percent of the organisation's global annual revenue from the preceding financial year, whichever is greater. Understanding the options to avoid running afoul of these data protection laws is essential. The DPF provides US organisations with a mechanism to demonstrate compliance with the GDPR and other data protection laws.

The DPF programme provides important benefits to US-based organisations as well as to their partners in Europe. The EU-US DPF, the UK Extension to the EU-US DPF and the Swiss-US DPF will be recognised by the European Commission

(EC), the UK government and the Swiss Federal Administration as compliant with relevant EU, UK and Swiss data protection requirements applicable to transfers of personal data to the US in support of transatlantic commerce. Once such formal recognition enters into force, participating organisations will be deemed as providing adequate privacy protection, a requirement for the transfer of personal data outside of the EU under the GDPR, outside of the UK under the UK Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR), and outside of Switzerland under the Swiss Federal Act on Data Protection (FADP). Compliance requirements are clearly laid out and can be implemented by small and medium-sized enterprises.

"The DPF programme provides important benefits to US-based organisations as well as to their partners in Europe."

How do US organisations participate in the DPF?

The DPF programme, administered by the International Trade Administration (ITA) within the US Department of Commerce, enables eligible US-based organisations to self-certify their compliance pursuant to the various DPF programmes. To participate in the DPF programme, a US-based organisation is required to self-certify to the ITA via the Department's DPF programme website and publicly commit to comply with DPF principles. While the decision by an eligible US-based organisation to self-certify its compliance pursuant to and participate in the relevant parts of the DPF programme is voluntary, effective compliance upon self-certification is compulsory. Once such an organisation self-certifies to the ITA and publicly declares its commitment to adhere to DPF principles, that commitment is enforceable under US law.

To rely on the EU-US DPF and, as applicable, the UK extension to the EU-US DPF or the Swiss-US DPF, an organisation must self-certify its adherence to DPF principles to the ITA and be placed and remain on the Data Privacy Framework List. The ITA will update this list based on annual recertification submissions

made by participating organisations and removing organisations when they voluntarily withdraw, fail to complete the annual recertification in accordance with the ITA's procedures or are found to persistently fail to comply. The ITA will also maintain and make available to the public an authoritative record of US organisations that have been removed from the Data Privacy Framework List and identify the reason each organisation was removed. The aforementioned authoritative list and record will remain available to the public on the US Department of Commerce's DPF programme website.

What are the key steps to joining?

Confirm your organisation's eligibility to participate in the DPF programme. Only US legal entities subject to the jurisdiction of the Federal Trade Commission (FTC) or the US Department of Transportation (DOT) are currently eligible to participate in the DPF programme. In order to be transferred in reliance on parts of the DPF programme, personal data must be processed in connection with an activity that is subject to the jurisdiction of at least one appropriate statutory body listed in the DPF principles.

Make specific reference in the privacy policy to your organisation's compliance with the DPF principles. Organisations must develop a DPF-compliant privacy policy before submitting their initial self-certification to the ITA and ensure it conforms to DPF principles. Among other things, the privacy policy should reflect organisations' information-handling practices and the choices it offers individuals with respect to the use and disclosure of their personal information. It is important to write a policy that is clear, concise and easy to understand.

Additional steps. Organisations need to identify their independent recourse mechanisms (IRMs), outlined below. The full list of steps to join the programme can be found on the DPF programme website.

What are the rights of nationals from participating countries pursuant to the DPF?

A participating organisation must provide, among other requirements: (i) information on the types of personal data collected; (ii) information on the purposes of collection and use; (iii) information on the type or identity of third parties to which personal data is disclosed; (iv) choices for limiting use and disclosure of personal data; (v) access to personal data; (vi) notification of the organisation's liability if it transfers personal data; (vii) notification of the requirement to disclose personal data in response to lawful requests by public authorities; (viii) reasonable and appropriate security for personal data; (ix) a response to your complaint within 45 days; (x) cost-free independent dispute resolution to address data protection concerns; and (xi) the ability to invoke

binding arbitration to address any complaint that the organisation has violated its obligations under the DPF principles and that has not been resolved by other means.

ICDR role

The ICDR, the international division of the American Arbitration Association, plays a critical role in the DPF.

The ICDR is available as an independent recourse mechanism for the DPF programme. The DPF requires participating organisations to provide – at no cost to the individual – an IRM to investigate and expeditiously resolve each individual's complaints and disputes. The IRM is a free and confidential service that provides EU, Swiss and UK individuals with a way to resolve disputes with US organisations regarding the handling of their personal data. To meet this requirement, an organisation may choose an ADR provider, such as the ICDR, to resolve its disputes.

The ICDR was selected by the US Department of Commerce to administer arbitrations pursuant to and to manage the arbitral fund identified in annex I of the DPF principles. In annex I of the EU-US DPF principles, the US Department of Commerce committed to facilitating the establishment of a fund into which participating organisations will be required to pay contributions to cover the arbitral cost, including arbitrator fees up to maximum amounts, in consultation with the EC. The purpose of the fund is solely to provide participating organisations with a consolidated mechanism to fund the annex I arbitrations.

The ICDR is the exclusive administrator for the EU-US DPF annex I binding arbitration programme. The ICDR provides dispute resolution services around the world and incorporates best international arbitration practices designed to deliver fair, efficient and economic proceedings. In cooperation with the US Department of Commerce and the EC, the ICDR has developed arbitration rules for EU-US DPF annex I arbitrations. These rules incorporate the required terms contained within the EU-US DPF principles and annex I of the DPF principles. This final and binding arbitration mechanism is in place to resolve any residual claims not resolved by the US organisation or through the IRM procedure, as well as any claim provided to the US Department of Commerce through the claimant's data protection authority and not resolved through best efforts within 90 days. CD

Luis M. Martinez
Vice President
International Centre for Dispute Resolution (ICDR)
T: +1 (212) 716 5833
E: martinezl@adr.org