Data Privacy Framework vs Standard Contractual Clauses

Requirement		Data Privacy Framework (DPF)[1]	Standard Contractual Clauses (SCC)
Eligibility		Organization must be subject to the investigation and enforcement powers of the **Federal Trade Commission (FTC)** or **Department of Transportation (DoT)**.	The SCCs can be used by controllers or processors that are subject to the GDPR to transfer personal data to controllers or processors outside the EEA **whose activities are not subject to the GDPR**.
Application		EU-U.S. personal data transfers only. [2]	EEA, Swiss and UK[3] transfers to whole world.
Principles	**Notice**	A DPF organization must have a privacy notice that includes an extensive list of information.	The data importer must inform the data subject, directly or through the exporter of a **more limited list** of information.
	Choice	Data subjects have the right to: • Opt out of use of data for marketing purposes • Opt out of personal data being disclosed to a third party[4] or used for a purpose that is materially different from the purposes for which it was originally collected • Opt in to sensitive personal data being disclosed or used as stated above	Data subjects have the right to: • Opt out of use of data for marketing purposes • Not be subject to fully automated decision-making, except under certain conditions and subject to specific safeguards
	Onward transfers	**By all organizations:** To controllers: Organizations must enter into a contract that states (i) data must only be processed for limited and specified purposes; (ii) the recipient will provide the same level of protection as the principles; and (iii) will notify the organization if it can no longer meet these obligations. To processors: Organizations must enter into a contract that stipulates the same as (i)–(iii) above, and (iv) to take steps to remediate any unauthorized processing.	**By controller importer:** Importers may only make an onward transfer if the recipient of the onward transfer agrees to be bound by the SCCs or if certain other grounds are met, the parties enter into a binding instrument, it is necessary for legal claims or vital interests, or based on explicit consent of the data subject. **By processor importers:** Importers may only make an onward transfer on the instructions of the exporter. Processor cannot rely on binding instruments or explicit consent of the data subject.
	Security	Organizations must take **reasonable and appropriate** measures to protect data from loss, misuse, unauthorized access, disclosure, alteration and destruction.	Importers need to **take appropriate** technical and organizational measures. Measures need to be included in the SCCs.
	Data minimization	Data minimization principle **applies** to the organization.	Data minimization principle **applies** to controller importers.
	Purpose limitation	Purpose limitation principle **applies** to the organization.	Purpose limitation principle **applies** to all data importers.
	Accuracy	Accuracy principle **applies** to the organization.	Accuracy principle **applies** to controller data importers.

1 Please note that where the self-certifying organization is receiving personal data as a processor, the exporter and such processor will still need to enter into a data processing agreement that complies with Article 28 GDPR.
2 Although there are UK and Swiss extensions to the DPF, these have not yet been recognized by the UK or Swiss authorities, respectively, as adequate.
3 For the UK, the UK Addendum needs to be added.
4 Does not apply to disclosures to processors.

Data Privacy Framework vs Standard Contractual Clauses

Access requests by public authorities	To the extent legally permissible, organizations may issue **periodic transparency reports** on the number of requests for data received from public authorities for law enforcement or national security purposes. Absence of a disclosure in the privacy policy does not preclude the organization from responding to such requests.	Importers must promptly **notify** the exporter and data subjects of any public authority access request and **review the legality** of such requests.
Access requests from data subjects	Organization must respond to an access request except in limit situations.	Controller importers must comply with access requests except in limited situations. Processor importers are only required to notify exporters of any access requests and assist with compliance.
Other rights for data subjects	Organization must respond to a request to correct, amend, or delete personal data where it is inaccurate or processed in violation of the principles.	Controller importers must comply with the following requests: rectification, erasure, option to object to processing for direct marketing purposes and option to consent to automated decision-making. Processor importers are only required to notify exporters of any requests and assist with compliance.
Data subject's ability to enforce	Data subjects will be able to enforce their rights by bringing a complaint directly to an organization, to an independent dispute resolution body in the United States or in the EU free of charge, either to an arbitration panel or to their national data protection authority in the EU.	Data subjects may enforce the clauses as third-party beneficiaries against the exporter and/or importer, except in relation to certain clauses (depending on the module used).
Audit rights	No right of audit for the exporter.[5]	Processor importers must allow for and contribute to audits of their processing activities at the exporter's request, at reasonable intervals or if there are indications of non-compliance.
Regulatory and judicial oversight and liability	The FTC and DoT will enforce the DPF. An organization's failure to abide by commitments to implement the DPF Principles may be challenged as deceptive by the FTC. The DoT has equivalent powers. An organization can be removed from the DPF List if it is found to have persistently failed to comply with the DPF Principles.	Importer agrees to submit to the jurisdiction of and cooperate with the competent EU supervisory authority and agrees to abide by a binding decision under applicable EU or member state law. Importer agrees to be liable for any damages it causes the data exporter, and to the data subject for any material and non-material damages that the importer causes in breaching any of the third-party beneficiary clauses.
Self-certification requirements	Yes. Refer to 'New privacy framework certification vs previous privacy shield certification' table.	Not applicable.
Transfer impact assessment (TIA)	A TIA is not required for transfers under the DPF.	A TIA is required.
HR data	Specific requirements apply to an organization's handling of HR data.	No specific requirements. Such data can be transferred under the SCCs.
Travel information	Specific requirements apply to an organization's handling of travel information.	No specific requirements. Such data can be transferred under the SCCs.
Pharmaceutical and medical products	Specific requirements apply to an organization's handling of personal data developed in specific medical or pharmaceutical research studies.	No specific requirements. Such data can be transferred under the SCCs.
Public record information	Certain principles do not apply to an organization's handling of public record information.	No specific requirements. Such data can be transferred under the SCCs.

ReedSmith

Driving progress
through partnership

5 Except where there is a controller–processor relationship, as a DPA will need to be put in place – see footnote 1.