LYDIAN

# DATA PRIVACY FRAMEWORK (DPF) – STANDARD CONTRACTUAL CLAUSES (SCC)

## AT-A-GLANCE COMPARISON

| | Data Privacy Framework (DPF) | Standard Contractual Clauses (SCC) |
|---|---|---|
| **Types of Transfers Covered** | **All Types of Transfers** – Covers controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller transfers. | **All Types of Transfers** – Covers controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller transfers. |
| **Personal Scope (Data Importer)** | **Limited** – Only U.S. organisations that are subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (***FTC***) or the U.S. Department of Transportation (***DoT***) can self-certify their commitment to adhere to the DPF.<br><br>This excludes, amongst others, banks, savings and loan institutions, federal credit unions and common carriers acting as U.S. Data Importers. | **Unlimited** – SCC can be used for transfers of personal data to any type of organisation acting as Data Importer. |
| **Material Scope** | **Any Personal Data** – Covers the transfer of any personal data to DPF-certified U.S. organisations, including HR-related data where so indicated in the self-certification of the U.S. Data Importer. | **Personal Data Described** – Only covers transfers of personal data as described in Annex 1 to the relevant/applicable SCC. |
| **Territorial Scope** | **U.S. Only** – Only covers transfers of personal data to the U.S., and, more particularly, to DPF-certified U.S. organisations. | **Rest of World** – May be used to ensure adequate safeguards for transfers to any country outside the European Economic Area (EEA) (including the U.S.). |

| | Data Privacy Framework (DPF) | Standard Contractual Clauses (SCC) |
|---|---|---|
| **Mechanism for Bindingness** | **Self-Certification** – Unilateral commitment vis-à-vis U.S. Department of Commerce (***DoC***) that the organisation acting as Data Importer shall comply with the Principles and the Supplemental Principles of the DPF. | **Contract** – Contractual commitment by Data Importer to comply with the obligations set out in the SCC (which differ depending upon the applicable Module). |
| **Reliance** | **Erga Omnes** – Any EU controller or processor transferring data to a DPF-certified U.S. organisation acting as Data Importer may rely upon the DPF.<br><br>*Note: data subjects derive their rights directly from the DPF (as well as the privacy policies adopted by the DPF-certified U.S. Data Importer pursuant to the DPF).* | **Contracting Data Exporter Only** – Only the EU controller or processor that entered into the SCC may rely upon the SCC.<br><br>*Note: data subjects may rely upon and invoke certain clauses of the SCC due to their status as third-party beneficiaries under Clause 3 of the SCC.* |
| **Data Transfer Impact Assessment (DTIA)** | **Not Required** – A DTIA is not required for transfers of personal data to DPF-certified U.S. organisations acting as Data Importer. | **Required** – A DTIA is required for (i) transfers of personal data to non-EEA countries that do not benefit from an adequacy decision and (ii) transfers of personal data to U.S. organisations that are not DPF-certified.<br><br>*Note: for transfers of personal data to U.S. organisations that are not DPF-certified, the European Commission's adequacy decision for the DPF and the Executive Order 14086 may be invoked to argue that the SCC will not be rendered ineffective by foreign (i.e., U.S.) law.* |
| **Supplementary Measures** | **Not Required** – It is not required for the Data Exporter and the Data Importer to agree upon supplementary measures (pursuant to EDPB Recommendation 01/2020). | **Sometimes Required** – Depending upon the outcome of the DTIA, the Data Exporter and the Data Importer may be required to agree on supplementary measures (pursuant to EDPB Recommendation 01/2020) (e.g., encryption with BYOK, etc.).<br><br>*Note: for transfers of personal data to U.S. organisations that are not DPF-certified, the European Commission's adequacy decision for the DPF and the Executive Order 14086 may be invoked to argue that the SCC will not be rendered ineffective by foreign (i.e., U.S.) law and that, as a result, there is no need to agree on supplementary measures.* |

| | Data Privacy Framework (DPF) | Standard Contractual Clauses (SCC) |
|---|---|---|
| **Transparency about the Transfer Mechanism (towards Data Subjects)** | **Privacy Statements** – Data subjects must be informed about the participation of the U.S. organisation in the DPF and its privacy statements reflecting the Principles (and Supplementary Principles) of the DPF must be made public (or, in the case of human resources data, be made readily available to the concerned individuals) and links to the U.S. Department of Commerce (***DoC***)'s website (with further details on certification, the rights of data subjects and available recourse mechanisms), the Data Privacy Framework List (***DPF List***) of participating organisations and the website of an appropriate alternative dispute settlement provider must be provided. | **Copy of the SCC** – On request, a copy of the SCC, including the Annexes – if needed, redacted to protect business secrets or other confidential information – must be made available to the data subject free-of-charge.<br><br>*Note: this transparency requirement does not apply to processor-to-controller (Module 4) transfers.* |
| **Onward Transfers** | **Restricted** – Any onward transfer by the Data Importer can only take place (i) for limited and specified purposes, (ii) on the basis of a contract between the DPF-certified U.S. organisation acting as Data Importer and the third party (or comparable arrangement within a corporate group) and (iii) only if that contract requires the third party to provide the same level of protection as the one guaranteed by the Principles (and Supplemental Principles) of the DPF. | **Restricted –** Other than in a limited number of exceptions such as the consent of the data subject, onward transfers by the Data Importer are only allowed to a party that is or agrees to be bound by the appropriate Module(s). |
| **Audit Rights for Data Exporter** | **No** – No audit rights foreseen for the Data Exporter. Compliance with the DPF is enforced by the U.S. Department of Commerce (***DoC***), the U.S. Federal Trade Commission (***FTC***) and the U.S. Department of Transport (***DoT***).<br><br>*Note: in case of controller-to-processor, processor-to-processor or processor-to-controller transfers, a processing agreement must be put in place (Art. 28 GDPR), which must (as always) provide for certain information and audit rights.* | **Yes** – Audit rights are foreseen for the Data Exporter in case of controller-to-processor (Module 2) and processor-to-processor (Module 3) transfers. |

| | Data Privacy Framework (DPF) | Standard Contractual Clauses (SCC) |
|---|---|---|
| **Formalities** | **No** – No further formalities need to be complied with by the Data Exporter and the Data Importer if the Data Importer is a DPF-certified U.S. organisation.<br><br>*Note: in case of controller-to-processor, processor-to-processor or processor-to-controller transfers, a processing agreement must (always) be put in place (Art. 28 GDPR).* | **Yes** – Data Exporter and Data Importer need to enter into (i.e., sign) the SCC, after having appropriately completed the SCC and having chosen the applicable Module(s).<br><br>*Note: in case of controller-to-processor, processor-to-processor or processor-to-controller transfers, the applicable Modules (2, 3 and 4) of the SCC already contain the requirements to comply with Art. 28 GDPR (obligation to put a processing agreement in place).* |
| **Periodical Review** | **Annual recertification** – The DPF-certified U.S. organisation is required to re-certify its adherence to the DPF on an annual basis. | **No –** Except in cases where new SCC are issued by the European Commission, there is no need to update the SCC once adopted.<br><br>*Note: in case of changes to the transfers or processing operations covered by the SCC, the SCC (more in particular, its Annexes) will need to be updated.* |
| **Enforcement** | **Supervision by U.S. Authorities** – Compliance with the DPF is enforced by the U.S. Department of Commerce (***DoC***), the U.S. Federal Trade Commission (***FTC***) and the U.S. Department of Transport (***DoT***). EU Supervisory Authorities have a limited role in enforcement of the DPF, although cooperation with EU DPAs is mandatory for organisations that process human resources data. | **Supervision by Data Exporter** – Compliance with the SCC is mainly enforced by the Data Exporter (through its contractual rights). Additionally, affected data subjects may enforce the SCC through their rights as third-party beneficiaries (Clause 3 of the SCC). EU Supervisory Authorities have a limited role in enforcement (given the contractual nature of the arrangement). |
| **Authorisation Supervisory Authority Data Exporter** | **No** – There is no need for approval by the Supervisory Authority of the Data Exporter. | **No** – There is no need for approval by the Supervisory Authority of the Data Exporter.<br><br>*Note: this only applies insofar the SCC entered into do not deviate from the text of the SCC adopted by the European Commission. Contractual safeguards that deviate from the SCC are considered 'ad hoc' contractual safeguards and are subject to the authorisation of the competent Supervisory Authority.* |

| | Data Privacy Framework (DPF) | Standard Contractual Clauses (SCC) |
|---|---|---|
| **Flexibility** | **Yes** – The DPF offers more flexibility as additional transfers (e.g., other purposes, other processing activities, other categories of personal data) do not require any further formalities.<br><br>*Note: where such additional transfer would involve HR data, then the scope of the Data Importer's DPF-certification needs to be checked to ascertain that HR data are included.* | **No** – Additional transfers not falling within the scope of Annex 1 of the SCC will require updating of the Annexes of to the SCC. Data Exporters are required to monitor additional transfers and may be required to regularly amend the SCC entered into.<br><br>In addition, the SCC must be implemented without changes (compared to the text of the SCC adopted by the European Commission). Contractual safeguards that deviate from the SCC are considered '*ad hoc*' contractual safeguards and are subject to the authorisation of the competent Supervisory Authority. |


Bastiaan Bruyndonckx
*Partner*
Information Governance & Data Protection (Privacy)
LYDIAN

bastiaan.bruyndonckx@lydian.be

Olivia Santantonio
*Counsel*
Information Governance & Data Protection (Privacy)
LYDIAN

olivia.santantonio@lydian.be

Liese Kuyken
*Associate*
Information Governance & Data Protection (Privacy)
LYDIAN

liese.kuyken@lydian.be