Sopra Steria Group

Group Data Protection Governance Model

October 2022

Table of Contents

Introduction

Sopra Steria Group is committed to protecting the privacy and security of personal information it holds and processes in accordance with applicable Data Protection laws, in particular with Regulation (EC) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("GDPR").

This Governance Model helps define Data Protection compliance goals and how they are set and achieved, specify authority and accountability for key roles, organize the reporting process to the Management team and an efficient structure for communication flow, establish an internal audit activity.

Thus, the Governance Model is a guidance system for both senior management and operational staff, made of standard management practices designed to suit the organization.

The Data Protection Governance Model is structured as follows:

- Framework for responsibility and accountability
- The Group Data Protection Compliance Program
- Annex 1 - Glossary

This Governance Model is applicable across all subsidiaries of Sopra Steria Group.

When reference is made in this document to "Sopra Steria Group" or "the Group", it should be noted that "Sopra Steria Group" or "the Group" coincides with the entity under French law "Sopra Steria Group SA" and not with a separate legal entity. Sopra Steria Group SA has both a corporate function, i.e., providing resources and guidance to all Sopra Steria subsidiaries, and a management function for business activities on the French territory.

1. Framework for Responsibility and Accountability

Along with the Group Data Protection Compliance program (Chapter 3), the underlying organizational structure that makes it actionable is outlined below. This management setup in charge of overseeing the execution of the Group Data Protection Governance Model is organized at multiple levels.

1.1. The Data Protection team at Group level

1.1.1. The Group Data Protection Officer (Group DPO)

The Group Data Protection Officer ("Group DPO") operates at a strategic level by providing guidance and support to DPOs and SPOCs appointed for each Sopra Steria subsidiary ("Local DPOs and SPOCs") who are responsible for compliance with data protection requirements within their respective entities. In this activity he/she is supported by the Group Privacy and Data Protection Governance Manager.

The Group DPO chairs the Data Protection Committee ("DPC", see section 1.1.3 below) in cooperation with the Group Privacy and Data Protection Governance Manager and instructs its participants on the actions to be undertaken to ensure regulatory compliance. Depending on the subject matter of discussion, the Group DPO may invite representatives of specific functions at Group level to attend the DPC.

1.1.2. The Group Privacy and Data Protection Governance Manager

The Group Privacy and Data Protection Governance Manager works in close cooperation with the Group DPO in defining the Group Data Protection Governance Model, establishing the compliance action plans and timeframes, ensuring harmonized compliance tools across all subsidiaries, monitoring correct application of the Data Protection Compliance program, organizing training sessions and providing guidance and support to Local DPOs and SPOCs. In addition, the Group Privacy and Data Protection Governance Manager acts as the Group SPOC for all privacy-related issues.

The Group Privacy and Data Protection Governance Manager chairs the DPC jointly with the Group DPO and is responsible for organizing monthly meetings with the Local DPOs/SPOCs (or their delegates) of Sopra Steria Group's subsidiaries. The monthly meeting has as its main objective to provide the Local DPOs/SPOCs with a recurring opportunity to:

- Share opinions, best practices, issues encountered in the privacy compliance exercise which can be of common interest, requests for intervention at Group level;
- Collect messages and requests to be conveyed to and discussed with the Group DPO in order to take necessary actions;
- Receive updates on ongoing initiatives at Group level;
- Get to know the other Local DPOs/SPOCs to intensify cooperation and get inspired from each other.

1.1.3. The Data Protection Committee (DPC)

The DPC is established at Group level to ensure the consistent application of the Group Data Protection Governance Model across all subsidiaries of Sopra Steria Group. The DPC is chaired by the Group DPO jointly with the Group Privacy and Data Protection Governance Manager. The DPC is made up of Local DPOs or SPOCs (or their delegates). Depending on the subject matter of discussion, the DPC may include representatives of specific functions at Group level.

The DPC is required to express its view on the proposed Data Protection documents (policies, procedures, guidelines etc.) and other initiatives (e.g., training courses).

The DPC shall meet at least once a year or more often if necessary.

1.2. The Data Protection team at Subsidiary level

1.2.1. The Local DPOs and SPOCs

A Local DPO is appointed for each Sopra Steria subsidiary (or group of subsidiaries within the same geography or sector) by the subsidiary/Controller concerned in consultation with the Group DPO. The Local DPO is responsible for ensuring the implementation of the Group Data Protection Compliance program and the respect by the subsidiary of applicable regulations and practices. When a Local DPO is not appointed, the subsidiary shall at least ensure the presence of a Data Protection SPOC within its organization.

More specifically, the Local DPO:

- is not hierarchically subordinate to the Group DPO, but has a duty to report to the latter on his/her actions and to escalate any difficulties encountered in implementing the compliance program, as well as any privacy-related issues, in particular personal data breaches;
- constantly liaises with Personal Data Owners (see Section 1.2.2 below) to provide guidance on how to implement the compliance program and has visibility on all processing operations carried out within the subsidiary.

The Local DPO shall inform the Group DPO of the notification of his/her official appointment to the competent Supervisory Authority (where applicable).

The Local DPO/SPOC must have expertise in national and European data protection laws and practices and a good understanding of the information systems and processing operations carried out within his/her subsidiary.

The position of the Local DPO within the organization:

a) **Independence**: he/she does not receive any instructions regarding the execution of his/her tasks, and he/she cannot be dismissed or penalized for his/her advice. He/she reports to the highest management level of the organisation;
b) **Centrality & Accessibility**: he/she should be effectively accessible meaning that he/she must be in a position to efficiently communicate with Data Subjects and cooperate with the competent Supervisory Authority. At the same time, he/she must be regularly in contact with the Personal Data Owners and the operational staff and be involved properly and in a timely manner in all issues related to the protection of personal data.

The tasks of the Local DPO are the following:

- **SPOC**: he/she acts as an intermediary between relevant stakeholders (e.g., Supervisory Authorities, Data Subjects, business units and other departments within the organization, Group DPO and Group Privacy and Data Protection Governance Manager);

- **Monitoring & Advice**: he/she assesses the *status quo* and fills the gaps in areas of non or partial compliance. He/she monitors compliance with applicable Data Protection laws and with the Group Data Protection Compliance program. He/she provides advice as regards DPIAs and monitors their performance. He/she implements and keeps up to date the necessary documentation to demonstrate compliance, especially records of data processing activities carried out within the organization. He/she follows Data Protection regulatory developments and gives recommendations about the interpretation or application of data protection rules. He/she checks staff completion of mandatory training courses and requires managers to urge their team members to complete them;
- **Awareness raising**: he/she is responsible to raise awareness among the staff involved in the processing of personal data, informs the subsidiary/Controller and its employees of their data protection obligations, trains and assigns responsibilities to his/her team members. Overall, he/she promotes a culture of data protection compliance across all units of the organisation;
- **Cooperation**: he/she liaises with other DPOs/SPOCs within the Group as well as with the Group DPO and the Group Privacy and Data Protection Governance Manager in order to exchange best practices and cooperate on issues of common interest. Also, he/she presents an annual report to both the general management of the subsidiary(ies) he/she belongs to and the Group DPO. At the end of his/her mission, he/she ensures handover to his/her successor.

1.2.2. Personal Data Owners

Personal Data Owners are reference persons within teams or departments (both at Corporate level and locally within the Sopra Steria subsidiary) who process personal data as part of their respective functions (e.g. HR, Marketing, Accounting).

Personal Data Owners are often entitled to grant access rights to and modify the data they handle, and are responsible for the quality, integrity, and protection of their personal data set.

Accordingly, Personal Data Owners shall make sure that the Data Protection Compliance Program and the instructions of the Group or Local DPO are followed within their area of responsibility at Corporate level or in the Sopra Steria subsidiary to which they belong.

Each subsidiary is responsible for designating the Personal Data Owners within its organisation.

2. The Group Data Protection Compliance Program

The Group Data Protection Compliance Program is the basic set of documents governing the way in which Sopra Steria Group and its subsidiaries will operate to ensure effective compliance with applicable Data Protection laws.

More specifically, the purpose of the Programme is to identify and harmonise the minimum content of the policies and practices that the Group and its subsidiaries must put in place to ensure the protection of the personal data they control (when acting as Data Controllers) or process on behalf of other Data Controllers (when acting as Data Processors).

The program is made of appropriate 1) information notices, 2) policies, 3) procedures, 4) tools and 5) contractual instruments that help operate in accordance with applicable Data Protection laws and regulations.

It is the responsibility of each subsidiary to inform its personnel where to find the relevant compliance tools and documents.

2.1. The information notices

Sopra Steria pays particular attention to the various types of information to be made available to Data Subjects and requires every subsidiary to put in place and made accessible all the necessary information notices described in more detail below.

2.1.1. Group General Data Protection Notice

The Group General Data Protection Notice describes the general principles established by Sopra Steria and its subsidiaries to ensure adequate protection of personal data when processing is necessary in the context of their activity.

The General Data Protection Notice applies by default to all processing operations carried out by Sopra Steria and its subsidiaries when they act both as Data Controllers and Data Processors. It shall be officially adopted by each Sopra Steria subsidiary and made available to the relevant Data Subjects.

The General Data Protection Notice establishes a data protection framework and refers to separate information notices that vary depending on the categories of relevant Data Subjects (employees, candidates, clients, suppliers, etc.). These specific information notices are developed at Group level but may provide for deviations at local level depending on the requirements of applicable local laws. These notices are described in more detail in the sections below.

2.1.2. Employee Information Notice

The Employee Information Notice is addressed to Sopra Steria employees including interns and freelancers and provides information regarding the collection and processing methods of their personal data as well as their rights relating to such processing activities when the Sopra Steria subsidiary processing the data acts as Data Controller.

The notice is a supporting document for Sopra Steria subsidiaries and must be adapted to the context of the local entity.

The Employee Information Notice must be communicated to the individuals at the time data is collected, meaning that it should be part of the on-boarding exercise for new employees.

2.1.3. Candidate Information Notice

The purpose of the Candidate Information Notice is to provide candidates (respondents to job offers published by Sopra Steria or spontaneous candidates) with information on the processing of their personal data carried out by the Sopra Steria subsidiary acting as Data Controller during the recruitment process (collection and

processing of CVs and other related information, interview reports, etc.) via any available channel (website, email, recruiting tools, professional social media such as LinkedIn etc.).

2.1.4. Client Information Notice

The purpose of the Client Information Notice is to provide Sopra Steria clients and prospects' contact persons with information regarding the collection and processing of their personal data by the relevant Sopra Steria subsidiary acting as Data Controller. Personal information (notably contact details such as name, professional e-mail, and telephone number) is collected for the purpose of establishing and maintaining business relationships for the offer and supply of products and services.

2.1.5. Supplier Information Notice

This Supplier Information Notice describes the conditions under which Sopra Steria collects and processes the personal data (notably contact data such as name, professional e-mail, and telephone number) of its Suppliers in the context of business interactions such as the purchase of products and services for its own procurement or on behalf of clients, and more generally for the management of its business relations.

2.1.6. Data Protection Notice for the Website

The Personal Data Protection Notice specific for the Website describes the methods for collecting, storing, and processing personal data through the Sopra Steria website, in particular when the end-users use some of the services offered online such as signing up to a newsletter, subscribing to an event or accessing and downloading online content.

The Personal Data Protection Notice includes a reference to the cookie policy which provides for a list of all cookies in use on the Sopra Steria website with details of each tracker made available to end users to provide them with information on the processing of their personal data when they visit the Sopra Steria domain.

2.2. Policies

2.2.1. Data Protection by Design and by Default Policy

Data Controllers are required under applicable Data Protection laws to implement (and periodically review) appropriate technical and organizational measures to ensure Data Protection by Design and by Default principles are complied with within the organization. Having these requirements correctly implemented means that data protection is embedded into the design and architecture of IT systems and business practices, therefore from the very beginning and as a default setting.

The Data Protection by Design and by Default Policy serves as a guide to the practical implementation of these principles. Privacy by Design is a holistic concept and approach that may be applied, from their initial implementation to all operations throughout the organization, including information technology, business practices, internal processes, physical design, and networked infrastructure. On the other hand, Privacy by Default requires that only personal data which is necessary for each specific and documented processing purpose is kept within the organization.

The Data Protection by Design and by Default Policy provides guidance on how to incorporate privacy protection principles throughout the entire lifecycle of the work carried out by Sopra Steria, whether it is an internal system or process, the design of a product to be placed on the market or a software development project for a client.

2.2.2. Data Retention Policy

The Data Retention Policy is a set of guidelines which defines, documents, and justifies storage periods for specific categories of personal data depending on the purpose of the processing and applicable local laws.

In addition, the policy provides guidance on how to technically delete or anonymize data and who is responsible for the deletion or anonymization process.

2.3. Procedures

2.3.1. Procedure for handling requests from Data Subjects

Applicable Data Protection laws grant Data Subjects several explicit rights. Individuals have the right to know what personal data concerning them is held by the Data Controller, the right to access their information at any time and to exercise other rights relating to the processing of their personal data.

The Procedure for handling requests from Data Subjects aims at governing:

- the overall management of requests by Data Subjects with regard to the exercise of their rights;
- the roles and responsibilities of Sopra Steria staff handling Data Subjects' requests;
- regulatory requirements and limits to the exercise of Data Subject rights;
- the process to be followed by Data Subjects to exercise their rights in practice against Sopra Steria.

This procedure applies to all personal data in respect of which Sopra Steria acts as Data Controller or Joint Controller. Where Sopra Steria is acting as Data Processor, it will comply with any agreement in place with the relevant Data Controller.

2.3.2. Personal Data Breach Management Procedure

The Personal Data Breach Management Procedure defines the process to be followed by the Sopra Steria subsidiary in the event that a personal data breach occurs or is suspected to have occurred. This procedure provides the necessary tools to:

- qualify the information security incident as a personal data breach (for information security incidents not qualified as personal data breaches, the Group Information Security Policies remain fully applicable);
- assess the severity of the personal data breach;
- assist the Local DPO/SPOC in advising the subsidiary regarding notification to 1) the competent authorities and/or the affected individuals, when the subsidiary acts as Data Controller with respect to the personal data involved in the security incident 2) the Data Controller, when the subsidiary acts as Data Processor with respect to the personal data involved in the security incident.

The procedure also provides instructions to quickly determine the necessary mitigation measures to be implemented in the event of a personal data breach.

The procedure stipulates that the Group DPO and the Group Privacy and Data Protection Governance Manager shall both be informed without delay by the Local DPO/SPOC of any identified or suspected personal data breach.

The Local DPO/SPOC may, where needed, request guidance to the Group DPO and the Group Privacy and Data Protection Governance Manager regarding the assessment of the severity of the breach, the necessary measures to be adopted to mitigate the impact thereof and the decision of whether it is necessary to notify the Data Protection Authority and, possibly, the Data Subjects.

Both the Group DPO and the Group Privacy and Data Protection Governance Manager shall be kept informed of any developments regarding the management of the breach, from the moment of detection until the closure of the file.

The procedure shall be adopted and implemented at local level.

In addition, the Local DPO/SPOC shall complete and keep updated the Register of Personal Data Breaches. The register is in Excel format and is made of two parts:

- Register of breaches when the SSG subsidiary is acting as Data Controller
- Register of breaches when the SSG subsidiary is acting as Data Processor

The Local DPO/SPOC must retain such record of Data Breaches for a minimum of five (5) years, unless otherwise required by applicable local law. The register duly completed shall be shared with the Group DPO upon request and in any case once a year.

2.4. The Compliance tools

2.4.1. Adequacy Corporate

The Group has made available to all subsidiaries an online platform – "Adequacy Corporate" - aimed at facilitating the implementation of data protection requirements and its easy management and maintenance over time.

One single software brings together all fundamental modules of data protection compliance including:

- Registers of processing operations for Controllers and Processors;
- Privacy impact assessments based on the EBIOS methodology;
- Action plan and tools to monitor compliance progress.

Administrator, Manager and User rights are managed by the Group Legal Department.

In principle, at local level only the DPO/SPOC is authorized to enter, modify and validate information in Adequacy Corporate, but access may be granted to other people within the organization (e.g., CISO, Personal Data Owners) depending on the internal structure and upon request to the Group DPO/Group Privacy and Data Protection Governance Manager.

In general, the Group Privacy and Data Protection Governance Manager acts as the administrator of the tool and SPOC with the software vendor.

2.4.2. Records of processing operations

The register of processing operations is a document with inventory and analysis purposes, which must reflect the reality of the personal data processing activities and flows within the organization.

The Controller register

The Controller register is an inventory of all the processing operations carried out on the personal data held and controlled by the Data Controller and for which the Data Controller defines purposes and means. The Controller register must reflect and be based on a mapping of actual data flows within the organisation. This mapping is kept up to date on a regular basis and meetings are held on a quarterly basis to identify new flows within the organisation and inform Local DPOs/SPOCs accordingly.

The Processor register

The Processor register is an inventory of processing operations carried out on behalf of the Data Controller.

The SSG subsidiary which has implemented Adequacy Corporate within its organisation may use the Controller and Processor' registers available on the platform to comply with the inventory obligation set out in the applicable Data Protection laws. Otherwise, the format of the register can be chosen freely by the subsidiary provided that it complies with the requirements of the applicable law.

Every six months, the Local DPOs/SPOCs must check the status of processing operations within their organisation, verify whether there are any new processing operations, update existing ones if necessary and update the Controller and Processor registers accordingly. To carry out this check, the Local DPO/SPOC may use questionnaires to be completed by the Personal Data Owners within the subsidiary. Every year, the Local DPO/SPOC must send to the Group DPO the list of the new processing operations identified during the reference period.

2.4.3. Data Protection Impact Assessment (DPIA)

In line with the requirements of applicable Data Protection laws, Sopra Steria conducts Data Protection Impact Assessments (DPIAs) when the processing of personal data may result in specific risks to the rights and freedoms of individuals.

For carrying out DPIAs Sopra Steria recommends the use of either:

- The Privacy Impact Assessment (PIA) tool developed by the French Supervisory Authority (CNIL);
- The DPIA module in Adequacy Corporate based on the EBIOS methodology (Expression of Needs and Identification of Security Objectives).

The above solutions are interoperable meaning that the DPIA report generated by one tool can be easily integrated into the other tool.

Sopra Steria periodically reviews its DPIAs and the processing activities it carries out, at least when there is a change in the risk posed by the processing and/or when using new technologies and the data processing is likely to result in a high risk to individuals.

EU (and UK) Data Protection Authorities published a list of processing activities triggering a mandatory DPIA as well as a list of processing operations exempt from that requirement following review by the European Data Protection Board (EDPB). The result of the assessment of whether a DPIA is necessary for a specific processing

operation as well as the outcome (report) of the DPIA for such processing operation (when a DPIA is mandatory or highly advisable) should be recorded in the Data Controller's register.

The execution of a DPIA requires advice from the Local DPO and signature at an appropriate level, e.g., the BU Director.

2.4.4. Methodology for performing Data Transfer Impact Assessments (DTIA)

When personal data is transferred to a country outside the EEA not declared as offering an adequate level of protection by the European Commission – therefore not benefitting from an Adequacy Decision ("third country") - the Data Exporter must perform a Data Transfer Impact Assessment (DTIA) before undertaking such data transfer (see section 2.5.2). To enable its subsidiaries to perform the DTIA, the Group has made available a specific methodology which:

- allows to logically assess the safeguards available when transferring personal data to third countries and whether such safeguards are adequate in the specific context;
- consents the creation of a report of the assessed transfer that can be made available to the competent Supervisory Authority upon request.

2.5. Contractual instruments

2.5.1. Processing of personal data by Controllers and Processors subject to the EU GDPR

a. Data Processing Agreement (DPA) with Sopra Steria acting as Data Controller

The Group has drafted and made available a DPA template to be used to define the conditions under which a third-party entity (such as a subcontractor, supplier etc.) may process personal data on behalf of Sopra Steria Group SA or one of its subsidiaries (Data Controller) in the context of processing activities subject to the EU GDPR. The DPA template (SSG as Data Controller) is available to Local DPOs/SPOCs.

b. Data Processing Agreement (DPA) with Sopra Steria acting as Data Processor

The Group has drafted and made available a DPA template to be used to define the conditions under which Sopra Steria Group SA or one of its subsidiaries may process personal data on behalf of a Data Controller (notably a client) in the context of processing activities subject to the EU GDPR. The DPA template (SSG as Data Processor) is available to Local DPOs/SPOCs.

2.5.2. Restricted International Data Transfers (to Controllers or Processors outside the EEA whose activities are not subject to the EU GDPR)

When personal data is transferred to data controllers or processors based in a third country, additional safeguards and conditions must be imposed on those entities receiving the data to enable compliance with applicable Data Protection laws.

Standard Contractual Clauses (SCCs) approved by the European Commission are one of the ways set out in the EU GDPR to transfer personal data to third countries in a sufficiently protective manner (also for transfers from the UK, since the UK has endorsed the SCCs as a transfer mechanism, albeit with some formal

adjustments according to its domestic law through the International Data Transfer Addendum (UK IDTA) to be attached to the EC SCCs). Binding Corporate Rules (BCRs) may also be used as a transfer mechanism to ensure international data flows comply with EU data protection standards. However, both SCCs and BCRs alone are not sufficient to secure data transfers and require carrying out a Data Transfer Impact Assessment (DTIA) which is an analysis of the conditions of the specific transfer in the context of legislation of the third country where the data importer is located. Based on the assessment, a decision is to be made regarding the adoption of adequate supplementary measures to carry out the transfer safely.

Below the steps to follow when considering transferring personal data to a third country:

1. Qualify the transfer and choose the applicable Data Transfer Agreement template incorporating the relevant module of the SCCs (where BCRs are not in place);
2. Assess if there is anything in the law or practices in force in the third country that may compromise the effectiveness of the safeguards contained in the SCCs/BCRs. This assessment should be focused on third country legislation;
3. Carry out the Data Transfer Impact Assessment (DTIA);
4. Adopt supplementary measures if necessary;
5. Sign the template incorporating the relevant module of the SCCs with description of supplementary measures, where necessary. Where BCRs are in place, describe the additional measures in a specific annex to be attached to the BCRs.

The explanatory note on the above steps and the webinar on the DTIA methodology are available to Local DPOs/SPOCs and their teams.

The following is a list of possible international data transfer scenarios that may occur within the Sopra Steria Group and the applicable transfer mechanisms:

- Personal data controlled by a Sopra Steria subsidiary subject to the EU GDPR (Data Controller) is transferred to another subsidiary based in a third country. Applicable transfer mechanisms:
  - Intra-group International Data Transfer Agreement (see paragraph a) below)
  - Controller BCRs (see paragraph b) below)
- Personal data controlled by a Sopra Steria subsidiary subject to the EU GDPR is transferred to an external entity based in a third country (acting as a separate Controller or Processor). Applicable transfer mechanisms:
  - Data Transfer Agreement incorporating the EC Standard Contractual Clauses (Controller to Controller or Controller to Processor) (see paragraph c) below)
- Personal data controlled by an external entity (notably a client) is transferred to a Sopra Steria subsidiary based in a third country acting as a Data Processor. Applicable transfer mechanisms:
  - Data Transfer Agreement incorporating the EC Standard Contractual Clauses (Controller to Processor) (see paragraph c) below)
  - Processor BCRs (see paragraph b) below)

- Personal data controlled by an external entity (notably a client) is transferred to a Sopra Steria subsidiary subject to the EU GDPR and acting as a Data Processor, which in turn transfers such data to a subsidiary based in a third country acting as a Sub-processor. Applicable transfer mechanisms:
  - Controller to Processor DPA and Intra-group International Data Transfer Agreement.

a. Intra-group International Data Transfer Agreement (IDTA)

For transfers to third countries of personal data subject to applicable EEA and UK Data Protection laws within the Sopra Steria Group, an Intra-group International Data Transfer Agreement (IDTA) is entered into between Sopra Steria Group SA and all its subsidiaries.

The IDTA consists of a multilateral framework agreement governing arrangements under which Sopra Steria subsidiaries transfer personal data between them where the transfers might otherwise be restricted by Applicable EEA and UK Data Protection Laws.

The IDTA also establishes Data Processing terms meeting the requirements of Article 28 EU GDPR/UK GDPR where one subsidiary processes personal data on behalf of another subsidiary.

b. Binding Corporate Rules (BCRs)

BCRs are legally binding and enforceable internal rules and policies for data transfers within multinational group companies and work in a way somewhat similar to an internal code of conduct. BCRs allow multinational companies to transfer personal data internationally within the same corporate group to countries that do not provide an adequate level of protection of personal data as required under the EU GDPR.

Having BCRs in place means establishing a harmonized data privacy standard across the international group. Although BCRs are designed as an international data transfer instrument, their scope is broader as they introduce a company-wide data privacy governance and policy framework binding upon all group companies "by design".

Within the Sopra Steria Group, only Sopra HR Software Group (SHRS) has adopted Controller and Processor BCRs after approval by the CNIL. BCRs govern data transfers from SHRS controllers and processors established in the EEA to other SHRS entities acting as controllers or internal processors/sub-processors established outside the EEA.

Significant changes to the SHRS BCRs or to the list of BCRs members are notified to all SHRS group members and to the competent Supervisory Authorities. Any significant changes to the SHRS BCRs must be communicated to Data Subjects as well. Certain modifications will also require a new authorization from the CNIL.

c. Data Transfer Agreements (DTA) incorporating the Standard Contractual Clauses (SCCs) of the European Commission

For international transfers which do not involve intra-group data flows, such as:

- Transfers of personal data controlled by a Sopra Steria subsidiary to an external entity based in a third country (acting as a separate Controller or Processor),
- Transfer of personal data controlled by an external entity (notably a client) to a Sopra Steria subsidiary based in a third country which acts as a separate Controller or Processor,

Data Transfer Agreement templates incorporating the SCCs of the European Commission (Controller to Controller, Controller to Processor, Processor to Sub-processor and Processor to Controller) are made available to Local DPOs/SPOCs. Below an overview of the available contractual templates:

I. *Data Transfer Agreement incorporating the SCCs applicable to transfers from a Controller (EU/EEA) to another Controller (non-EU/EEA)*
   - A Controller based in the EEA transfers personal data to another Controller based in a third country (two separate controllers).

II. *Data Transfer Agreement incorporating the SCCs applicable to transfers from a Controller (EU/EEA) to a Processor (non-EU/EEA)*
   - A Controller based in the EEA transfers personal data to a Processor based in a third country.

III. *Data Transfer Agreement incorporating the SCCs applicable to transfers from a Processor (EU/EEA) to a Sub-Processor (non-EU/EEA)*
   - A Processor based in the EEA transfers personal data to a Sub-processor based in a third country.

IV. *Data Transfer Agreement incorporating the SCCs applicable to transfers from a Processor (EU/EEA) to a Controller (non-EU/EEA)*
   - A Processor based in the EEA transfers personal data to a Controller based in a third country.

For guidance on how to use the templates, please refer to the explanatory note available to Local DPOs/SPOCs and their teams.

Once a year, the Local DPOs/SPOCs shall send to the Group DPO the list of international data transfers performed by their subsidiary in the context of the execution of service contracts.

3. Staff training and awareness

Sopra Steria requires all its employees to attend mandatory general training sessions on data privacy and security. Training sessions will be organized as often as necessary to ensure that Sopra Steria employees are kept properly informed of any obligations under applicable Data Protection laws as well as of any relevant regulatory changes and have clear understanding and awareness of Sopra Steria policies and procedures in place.

3.1. Staff training

3.1.1. Newcomers on-boarding day: presentation of Sopra Steria Data Protection rules and mandatory training

During the first days of employment, the HR team shall make sure the new employee is well aware at least of:

1. the Data Protection policies and procedures in place within the organization and where to find them;
2. the mandatory Data Protection e-learning module and deadlines for completion.

The Local DPOs/SPOCs are responsible for ensuring that all new employees in their subsidiary have successfully completed the Data Protection e-learning module within 3 months of their arrival. They are therefore

responsible for carrying out checks on a regular basis. Accordingly, the Local DPOs/SPOCs will report completion rate data back to the management team and urge Directors to request their team members to complete it. Any non-compliance is reported to the Group DPO.

Any employee may have access to the Data Protection e-learning module and related documentation at any time.

3.1.2. Specific Data Protection training

Each employee has the right to ask his or her manager to attend specific data protection training courses (depending on his or her specific role within the company). In this case, the manager should contact the Local DPO/SPOC.

3.2. Awareness raising

3.2.1. The Group Data Protection Day

In 2006 the Council of Europe decided to launch a Data Protection Day to be celebrated each year on 28 January, the date on which the Council of Europe's Data Protection Convention, known as "Convention 108", was opened for signature. The Data Protection Day is now celebrated globally and is called Privacy Day outside Europe.

Sopra Steria has decided to make the 28 January a day to be celebrated internally as well for the purpose of raising awareness on the importance of personal data protection among its employees. On this day, some awareness-raising activities will be organized at Group level: these may include campaigns targeting specific employees' groups, educational projects, quizzes, and lotteries.

3.2.2. The Sopra Steria Group Monthly Privacy Digest

The Group Privacy and Data Protection Governance Manager is responsible for the creation and recurrent dissemination to Local DPOs/SPOCs of a privacy newsletter that gathers news from EU Supervisory Authorities, the ICO, the European Data Protection Board and the European Data Protection Supervisor and provides updates on Group's action on privacy matters.

4. Practicalities

4.1. Compliance checklist and audit missions

4.1.1. Compliance checklist and Group DPO assessment

A checklist of minimum compliance policies, tools, and procedures that every Sopra Steria subsidiary needs to have in place to ensure an acceptable level of alignment with the Group Data Protection Compliance Program is made available to Local DPOs/SPOCs. These latter are in charge of communicating the documents of the

checklist that they have already adopted at local level. The checklist and the existing documents must be sent to the Group DPO for assessment once a year in the first quarter. The aim of the checklist assessment is to identify gaps between what has been implemented at local level and the minimum standards required by the Group and undertaking corrective actions where needed. The Group DPO may carry out on-site checks based on the results of the checklist assessment.

4.1.2. Audit Missions

The Internal Audit department is in charge of organizing audit activities on the progress and implementation of the Data Protection Compliance program at Group and local level according to the Group audit plan.

The audit missions will produce audit reports with an indication of corrective actions to be undertaken.

Annex 1 – Glossary

"Data Exporter": a Controller or Processor located within the EEA/UK that makes a Restricted International Transfer.

"Data Importer": a Controller or Processor located in a non-adequate third country, receiving personal data from the Data Exporter in the context of a Restricted International Transfer.

"Data Protection Committee (DPC)": a committee established at Group level to ensure the consistent application of the Group Data Protection Governance Model across all subsidiaries of the Sopra Steria Group, chaired by the Group DPO jointly with the Group Privacy and Data Protection Governance Manager, and made up of Local DPOs or SPOCs (or their delegates). Depending on the subject matter of discussion, the DPC may include representatives of specific functions at Group level.

"Data Transfer Agreements (DTA) incorporating the Standard Contractual Clauses (SCCs) of the European Commission": contractual templates incorporating the different modules of the SCCs (Controller to Controller, Controller to Processor, Processor to Sub-processor and Processor to Controller) to be used in the context of international data transfers that are not exclusively intra-group, but where the Data Exporter or the Data Importer is an entity external to Sopra Steria.

"Data Transfer Impact Assessment Methodology": process to be followed to perform Data Transfer Impact Assessments (DTIA). DTIA must be performed by the Data Exporter when personal data is transferred to a third country (outside the EEA) and this third country is not declared as offering an adequate level of protection by the European Commission. The methodology is made available by the Group to all Local DPOs and SPOCs.

"EEA": the European Economic Area.

"Framework for responsibility and accountability": the organizational structure at Group and subsidiary level in charge of implementing and overseeing the execution of the Group Data Protection Governance Model.

"Group Data Protection Compliance Program": the basic set of documents governing the way in which Sopra Steria Group and its subsidiaries will operate to ensure effective compliance with applicable Data Protection laws. More specifically, the purpose of the Programme is to identify and harmonise the minimum content of the policies and practices that the Group and its subsidiaries must put in place to ensure the protection of the personal data they control (when acting as Data Controllers) or process on behalf of other Data Controllers (when acting as Data Processors).

"Group Data Protection Governance Model": a harmonised guidance system for senior management and operational staff, applicable to all Sopra Steria Group subsidiaries, which defines the data protection compliance objectives and how they are set and achieved, specifies the authority and responsibility of key roles, organises the reporting process to the management team and an efficient structure for the flow of communication, and establishes internal audit activity.

"Group Data Protection Officer": the data protection leadership role at Group level, operating at the strategic level by providing guidance and support to Local DPOs and SPOCs.

"Group Privacy and Data Protection Governance Manager": the person who acts as the Group SPOC for all privacy-related issues and who is responsible, in cooperation with the Group DPO, for defining the Group Data Protection Governance Model, establishing the compliance action plans and timeframes, ensuring harmonized compliance tools across all subsidiaries, monitoring correct application of the Data Protection Compliance program, organizing training sessions and providing guidance and support to Local DPOs and SPOCs.

"Intra-group International Data Transfer Agreement (IDTA)": framework agreement which governs arrangements under which Sopra Steria subsidiaries may transfer personal data between them where the transfers might otherwise be restricted by Applicable EEA and UK Data Protection Laws, and which establishes data processing terms meeting the requirements of Article 28 EU GDPR/UK GDPR where one subsidiary processes personal data on behalf of another subsidiary.

"Local DPO": data protection expert appointed for each Sopra Steria subsidiary (or group of subsidiaries within the same geography or sector) by the subsidiary/Controller concerned in consultation with the Group DPO. The Local DPO is responsible for ensuring the implementation of the Group Data Protection Governance Model and the respect by the subsidiary of applicable regulations and practices.

"Local SPOC": a person within the Sopra Steria subsidiary who handles requests and queries and acts as an intermediary between stakeholders (e.g., supervisory authorities, data subjects, business units and other departments within the organisation, the Group DPO and Group Privacy and Data Protection Governance Manager, other Local DPOs and SPOCs) on privacy issues, when a DPO is not formally appointed.

"Personal Data Owners": reference persons within teams or departments (both at Corporate level and locally within the Sopra Steria subsidiary) who process personal data as part of their respective functions (e.g. HR, Marketing, Accounting), and who, by virtue of their role, are responsible for ensuring that the Data Protection Compliance Program as well as the Group and Local DPO's instructions are followed within their area of responsibility.

"Restricted International Transfer": international transfer of personal data that would be prohibited under applicable EEA Data Protection Laws or applicable UK Data Protection Laws in the absence of the protection for the transferred personal data provided by the SCCs or other transfer mechanism.

"Sopra Steria Group": (or "the Group") the entity under French law "Sopra Steria Group SA" which has both a corporate function, i.e., providing resources and guidance to all Sopra Steria subsidiaries, and a management function for business activities on the French territory.

"Sopra Steria Subsidiary": any company owned or controlled by Sopra Steria Group SA within the meaning of Article L 233-3 of the French Commercial Code.

"Third Country": any country which is not an EEA Member State, and not offering an adequate level of protection within the meaning of Article 45(1) of the EU GDPR.

"UK IDTA": the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A (1) Data Protection Act 2018.