Transborder Data Processing and Country Required Terms of the IBM DPA

The Transborder Data Processing and Country Required Terms (CRT) form part of the DPA and DPA Exhibit.

This document is divided into, (i) Section 1. Transborder Data Processing, which apply where there is a transfer of Client Personal Data to Non-Adequate Countries, as per the applicable Data Protection Laws requirements and (ii) Section 2. CRT, which apply where the parties are subject to additional country required terms, as per the applicable Data Protection Laws requirements.

In case of conflict between the Transborder Data Processing, the CRT and the DPA and/or DPA Exhibit, the respective Transborder Data Processing and CRT will prevail.

Capitalized terms used and not defined in the DPA have the meanings given to them by the applicable Data Protection Laws.

Contents

1. The Transborder Data Processing

a. In certain cases, and as per Data Protection Laws requirements, Client and IBM need to enter into specific transfer mechanisms for the transfer of Client Personal Data to Non-Adequate Countries. Those transfer mechanisms are listed below.

b. Only the relevant Transborder Data Processing will apply to Client and IBM, in accordance with the Agreement and the applicable Data Protection Laws.

c. IBM will enter into the standard contractual clauses for the transfer of Client Personal Data required by the applicable Data Protection Laws with each Subprocessor located in a Non-Adequate Country, as identified in the applicable DPA Exhibit.

d. Client agrees that the applicable standard contractual clauses, including any claims arising from them, are subject to the terms set forth in the Agreement, including the limitations of liability. In case of conflict, the provisions of the applicable standard contractual clauses shall prevail.

e. If required by the applicable Data Protection Laws, Client shall obtain consent from the Data Subjects for the transfer of Client Personal Data to Non-Adequate Countries.

1.1 The EU Standard Contractual Clauses

a. The EU Standard Contractual Clauses (meaning the standard contractual clauses as approved by EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (as amended or supplemented from time to time) (EU SCC)) apply to the Processing of Client Personal Data subject to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), where Client, IBM, or both are located in Non-Adequate Countries.

b. If the EU SCC are not required pursuant to the GDPR because both parties are located in a country providing an adequate level of protection, the EU SCC will become applicable if during the Service the country where IBM or Client is located becomes a Non-Adequate Country.

c. Section 1.c. applies, unless Subprocessor is already using an approved alternative transfer mechanism pursuant to Chapter V GDPR.

d. The EU SCC are incorporated by reference, as available on the EU Commission website. The EU SCC and its Appendix are completed as below. The parties acknowledge that the applicable module of the EU SCC will be determined by their respective role(s) as Controller and/or Processor under the circumstances of each transfer and are responsible for determining the correct role(s) undertaken to fulfil the appropriate obligations under the applicable module.

Section Reference	Concept	Selection by the Parties
Section I, Clause 7	Docking Clause	The optional Docking Clause shall not apply
Section II, Clause 9	Approval of Subprocessors	Option 2: General Written Authorization shall apply in accordance with the notification period set out in Section 7 of the DPA
Section II, Clause 11	Redress	The optional language shall not apply
Section II, Clause 13	Supervision	All options under Clause 13 (a) shall apply
Section IV, Clause 17	Governing law	Option 1: The law of the EU Member States where the competent supervisory authority is located according to Clause 13, unless such law does not allow for third-party beneficiary rights, in which case the parties will cooperate to determine the applicable law of another EU Member State
Section IV, Clause 18 (b)	Choice of forum and jurisdiction	The courts of the EU Member State where the competent supervisory authority is located, according to Clause 13

Appendix of the EU SCC

ANNEX I

A. LIST OF PARTIES

MODULE ONE TO FOUR

Data exporter(s):

Name: The data exporter is an entity (Client) that has contracted with the data importer (IBM) for Services, unless both IBM and Client are located in a country considered to have an adequate level of data protection pursuant to Data Protection Laws or a decision of the responsible Supervisory Authority, in which case these Clauses are not required between IBM and Client.

MODULE FOUR: Transfer processor to controller: the data exporter is the entity (IBM) that has contracted with the data importer (Client) to provide the Services.

Address: As set out in the Transaction Document.

Contact person's name, position and contact details: As set out in the Transaction Document.

Activities relevant to the data transferred under these Clauses: As set out in the applicable Transaction Document.

Signature and date: By entering into the Agreement, Client is entering into these Clauses, unless both IBM and Client are located in a country considered to have an adequate level of data protection pursuant to Data Protection Laws or a decision of the responsible Supervisory Authority, in which case these Clauses are not required between IBM and Client.

Role (controller/processor): The role of Client as controller, processor or both is determined by the circumstances of each case and Client is responsible for determining the correct role undertaken in order to fulfil the appropriate obligations under the applicable module.

MODULE FOUR: Transfer processor to controller: the data exporter is the processor.

2. Data importer(s):

Name: The data importer is IBM if located in a Non-Adequate Country.

MODULE FOUR: Transfer processor to controller: the data importer is an entity (Client) that has contracted with the data exporter (IBM) for the Services.

Address: As set out in the Transaction Document.

Contact person's name, position and contact details: As set out in the Transaction Document.

Activities relevant to the data transferred under these Clauses: As set out in the applicable Transaction Document.

Signature and date: By entering into the Agreement, IBM is entering into these Clauses, provided IBM is located in a Non-Adequate Country.

Role (controller/processor): IBM acts as processor.

MODULE FOUR: Transfer processor to controller: the data importer is the controller.

B. DESCRIPTION OF TRANSFER

MODULE ONE TO FOUR

Categories of data subjects whose personal data is transferred:

The personal data transferred may concern the categories of data subjects set out in section "Categories of Data Subjects" in the DPA Exhibit applicable to the respective Services.

Categories of personal data transferred:

The personal data transferred may concern the categories of data set out in section "Types of Personal Data" in the DPA Exhibit applicable to the respective Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed organization training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

The personal data transferred may concern sensitive data set out in section "Special Categories of Personal Data" in the DPA Exhibit applicable to the respective Services. Where sensitive data are set out in the DPA Exhibit, the technical and organizational measures set out in section "Technical and Organizational Measures" of the DPA Exhibit include the applied restrictions and safeguards that fully take into consideration the nature of the sensitive data and the risks involved.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous.

Nature of the processing:

The nature of processing is set out in section "Processing Activities" of the DPA Exhibit applicable to the respective Services.

Purpose(s) of the data transfer and further processing:

The purpose(s) is/are to provide and secure the respective Services, or as otherwise set out in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The period for which the personal data will be retained is set out in section "Duration of Processing" of the DPA Exhibit applicable to the respective Services.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

The subject matter and nature of processing is set out in section “Processing Activities” or “Subprocessors” of the DPA Exhibit applicable to the respective Services. The duration of processing is set out in section “Duration of Processing” of the DPA Exhibit applicable to the respective Services.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE TO THREE

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority is identified in accordance with Clause 13 depending on where the data exporter is established or

data subject is located as determined by the circumstances of each case.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE TO THREE

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The technical and organizational measures are set out in section “Technical and Organizational Measures” of the DPA Exhibit applicable to the respective Services.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

The Services are designed to enable Client to deal with any enquiries and requests that a controller receives from a data subject related to the processing of her/his personal data and the exercise of her/his rights. If Client requires further assistance, IBM has implemented organizational measures to assist Client and Client may contact IBM at chiefprivacyoffice@ca.ibm.com.

ANNEX III - LIST OF SUB-PROCESSORS

MODULE TWO AND THREE

This Annex III does not apply if the general authorization specified in Section 7 “Subprocessors” of the IBM DPA applies. A list of the subprocessors authorized by Client at the execution of these Clauses is set out in section “Subprocessors” or sections “IBM Processing Locations” and “Third-Party Subprocessors” of the DPA Exhibit applicable to the respective Services. Intended changes to the list will be managed pursuant to Clause 9(a) of these Clauses and Section 7 of the IBM DPA.

1.1.1 Additional Safeguards to the EU SCC

a. In accordance with the July 16, 2020 decision of the Court of Justice of the European Union (CJEU) in Case C-311/18 Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, and without prejudice to any provisions of the DPA, IBM will undertake additional safeguards to secure Personal Data transferred on the basis of the EU SCC to Non-Adequate Countries whose laws are likely to have a substantial adverse effect on the level of data protection offered by the EU SCC and required under EU data protection law.

b. IBM will implement and maintain the technical and organizational measures, as specified in the applicable DPA Exhibit, such as encryption, access controls, or similar technologies, as applicable and agreed with the Client, to protect Client Personal Data against any processing for national security or other government purposes that are determined to be massive, disproportionate, or indiscriminate in a manner that goes beyond what is necessary in a democratic society, considering the type of processing activities and IBM's scope of responsibility.

c. For the purposes of safeguarding Client Personal Data when any government or regulatory authority requests access to such data, IBM has implemented and shall continue to comply with the provisions of the following documents which remain accurate and valid: "Letter to Our Clients About Government Access to Data" and available to Clients since its publication on March 14, 2014 ("Data Access Letter"); and "Law Enforcement Requests Transparency Report" ("Transparency Report").

d. In the event of any such request for access to Client Personal Data by a government or regulatory authority:

   (1) IBM will notify Client of such request to enable Client to take all necessary actions to communicate directly with the relevant authority and respond to such request.

   (2) If IBM is prohibited by law to notify Client of such request, it will make best reasonable efforts to challenge such prohibition and it commits to providing the minimum amount of information permissible when responding, based on a reasonable interpretation of the order.

   (3) IBM will provide to Client general information relative to any such request received from a government or regulatory authority during the preceding 12-month period.

1.1.2 The UK Addendum to the EU SCC

a. The Section 1.1 The EU Standard Contractual Clauses above and the United Kingdom's International Data Transfer Addendum to the EU SCC (together, the (UK Addendum to the EU SCC)) will be implemented for transfers to Non-Adequate Countries subject to the UK General Data Protection Regulation and where Client, IBM, or both are located in Non-Adequate Countries.

b. The UK Addendum to the EU SCC is completed as below and modifies the Section 1.1.d. above.

ico.
Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses - **VERSION B1.0, in force 21 March 2022.**

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The start date is the date on which the Parties agreed to enter this Addendum under the Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	**Full legal name:** The Exporter is an entity (Client) that has contracted with the Importer (IBM) for Services, unless both IBM and Client are located in a country considered to have an adequate level of protection pursuant to UK data protection law, in which case this Addendum is not required between IBM and Client. MODULE FOUR of EU SCCs (if applicable): Transfer processor to controller: the Exporter is the entity (IBM) that has contracted with the Importer (Client) to provide the Services. **Trading name (if different):** **Main address (if a company registered address):** As set out in the Transaction Document. **Official registration number (if any) (company number or similar** **identifier):** As set out in the Transaction Document or as included on an official company register.	**Full legal name:** The Importer is IBM if located in a country not considered to have an adequate level of protection pursuant to UK data protection law. MODULE FOUR of EU SCCs (if applicable): Transfer processor to controller: the Importer is an entity (Client) that has contracted with the Exporter (IBM) for the Services. **Trading name (if different):** **Main address (if a company registered address):** As set out in the Transaction Document. **Official registration number (if any) (company number or similar** **identifier):** As set out in the Transaction Document or as included on an official company register.
Key Contact	**Job Title:** As set out in the Transaction Document. **Contact details including email:** As set out in the Transaction Document.	**Job Title:** As set out in the Transaction Document. **Contact details including email:** As set out in the Transaction Document.
Signature (if required for the purposes of Section 2)	By entering the Agreement, Client (and if Module 4 of the EU SCC applies, IBM) is entering into this Addendum, unless both IBM and Client are located in a country considered to have an adequate level of protection pursuant to UK data protection law, in which case this Addendum is not required between IBM and Client.	By entering the Agreement, IBM (and if Module 4 of the EU SCC applies, Client) is entering into this Addendum, provided IBM (or Client if Module 4 applies) is located in a country not considered to have an adequate level of protection pursuant to UK data protection law.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: See Part 1 of this document for the version of the Approved EU SCCs to which this Addendum is appended to. Reference (if any): Other identifier (if any):

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Appendix of the EU SCCs to which this Addendum is appended to.

Annex 1B: Description of Transfer: See Appendix of the EU SCCs to which this Addendum is appended to.

Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: See Appendix of the EU SCCs to which this Addendum is appended to.

Annex III: List of Sub processors (Modules 2 and 3 only): See Appendix of the EU SCCs to which this Addendum is appended to.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

1.1.3 Swiss Amendments to the EU SCC

In case of a transfer of Client Personal Data subject to the Swiss Federal Act on Data Protection of 19 June 1992; as of September 1, 2023, its totally revised version of 25 September 2020 (FADP) where Client, IBM, or both are located in Non-Adequate Countries, the EU SCC included in Section 1.1 The EU Standard Contractual Clauses above apply, with the following amendments:

a. The Swiss Federal Data Protection and Information Commissioner (FDPIC) is the competent supervisory authority in accordance with Clause 13 and Annex I.C of the EU SCC;

b. The governing law in accordance with Clause 17 of the EU SCC shall be Swiss law in case the data transfer is exclusively subject to the FADP;

c. The term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 of the EU SCC; and

d. References to the GDPR in the EU SCC shall also include the reference to the equivalent provisions of the FADP (as amended or replaced).

1.1.4 Applicability of the EU SCC for other Data Protection Laws

The EU SCC apply to the Processing of Client Personal Data subject to any other Data Protection Laws endorsing the EU SCC as a transfer mechanism, or allowing the use of the EU SCC to the extent not in conflict with the respective model clauses requirements, where Client, IBM, or both are located in Non-Adequate Countries. In this case, the Section 1.1 The EU Standard Contractual Clauses above apply, with the following amendments:

a. The supervisory authority in accordance with Clause 13 and Annex I.C of the EU SCC shall be the competent supervisory authority as stated in the applicable Data Protection Laws;

b. The governing law in accordance with Clause 17 of the EU SCC shall be the applicable Data Protection Laws;

c. The choice of forum and jurisdiction in accordance with Clause 18 of the EU SCC shall be the one applicable under the applicable Data Protection Laws; and

d. Any references to the GDPR in the EU SCC shall also include the reference to the equivalent provisions of the applicable Data Protection Laws.

1.1.5 Additional Transborder Data Processing

a. The IBM Data Privacy Framework Policy available at: https://www.ibm.com/privacy/dataprivacyframework (Policy), applies to the Data Privacy Framework-Certified Services designated therein, where Personal Data is transferred to the United States from countries whose data protection laws recognize the Data Privacy Framework as a valid mechanism for cross-border transfers.

b. This Policy does not apply when Client chooses to have its offering Content processed in countries other than the United States.

1.2 The Serbian Law on Personal Data Protection (Serbian SCC)

a. The Serbian SCC apply to the Processing of Client Personal Data subject to the Law on Personal Data Protection (Zakon o zaštiti podataka o ličnosti; Official Gazette of the Republic of Serbia, no 87/2018) where Client, IBM, or both are located in Non-Adequate Countries.

b. By entering into the Agreement, Client is entering into the Serbian SCC as adopted by the "Serbian Commissioner for Information of Public Importance and Personal Data Protection", published at https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx to provide an adequate level of protection.

c. Information required to complete Appendices 1 to 8 of the Serbian SCC for the purpose of governing the transfer of Personal Data to a Non-Adequate Country can be found in the DPA and DPA Exhibit.

d. Upon request, IBM will provide a copy of the Serbian SCCs in the Serbian language signed by the IBM Data Importers and a courtesy translation in English. Please submit requests to ChiefPrivacyOffice@ca.ibm.com

1.3 The Japanese Act on the Protection of Personal Information (APPI)

a. In case of a transfer of Client Personal Data that is subject to APPI to a Non-Adequate Country, the parties agree that the DPA and its respective DPA Exhibit(s) apply as legitimate measures required for such transfer.

b. The parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the Client Personal Data by IBM prevent them from implementing their obligations under the DPA and applicable DPA Exhibit(s).

c. The parties agree to notify the other party if, after having agreed to the DPA and for the duration of the contract, a party has reason to believe that either party cannot comply with its obligation under the DPA. In which case, the parties will cooperate in good faith to identify appropriate measures to be adopted to address the situation. If no appropriate measures can be implemented, the parties will evaluate together whether to suspend the transfer of Client Personal Data.

1.4 The Turkish Law on the Protection of Personal Data (Turkish SCC)

a. The Turkish standard contractual clauses (as approved by the Turkish Personal Data Protection Board and published at https://www.kvkk.gov.tr (Turkish SCC)) apply to the Processing of Client Personal Data subject to the Law on the Protection of Personal Data no 6698 dated April 7, 2016, and its implementing regulations (Turkish Data Protection Law), where Client, IBM, or both are located in Non-Adequate Countries. The parties acknowledge that the applicable module of the Turkish SCC will be determined by their respective role(s) as Controller and/or Processor under the circumstances of each transfer and are responsible for determining the correct role(s) undertaken to fulfil the appropriate obligations under the applicable module.

b. For the purposes of Clauses 8 (Sub-Processors) and 10 (Redress) of the Turkish SCC, the options set forth under Section 1.1. d., Clause 9 and Clause 11 of the EU SCC apply respectively. Information required to complete the Appendix, Annexes I to III of the Turkish SCC can be found in the Appendix of the EU SCC.

1.5 The Saudi Arabia Personal Data Protection Law (SA SCC)

a. The Saudi Arabia standard contractual clauses (as approved by the Saudi Data and AI Authority (SDAIA) and published at https://sdaia.gov.sa/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx (SA SCC)) apply to the Processing of Client Personal Data subject to the Saudi Arabia Data Protection Law (meaning the Saudi Arabia Personal Data Protection Law issued pursuant to Royal Decree No. (M/19) dated 9/2/1443 AH, as amended from time to time, and its implementing regulations), where Client, IBM, or both are located in Non-Adequate Countries. The parties acknowledge that the applicable module of the SA SCC will be determined by their respective role(s) as Controller and/or Processor under the circumstances of each transfer and are responsible for determining the correct role(s) undertaken to fulfil the appropriate obligations under the applicable module.

b. Information required to complete the Appendices 1 to 3 of the SA SCC can be found in the Appendix of the EU SCC.

1.6 The Brazilian General Data Protection Law (Brazilian SCC)

a. The Brazilian standard contractual clauses, as adopted by the National Data Protection Authority under Resolution n. 19/2024 and its Annex II of August 23,2024 (Brazilian SCC), apply to the Processing of Client Personal Data subject to the Brazil General Data Protection Law (Federal Law n. 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – (LGPD)) where Client, IBM, or both are located in Non-Adequate Countries. The parties acknowledge that their respective roles as Controller and/or Processor will be determined based on the circumstances of each transfer.

b. Information required to complete Clauses 1. (Identification of the Parties) and 2. (Object) of the Brazilian SCC is provided in the Appendix of the EU SCC. The designated contact for data subjects is the contact person specified in the relevant Transaction Document. For the purposes of Clause 3 (Onward Transfers) of the Brazilian SCC, Option B applies and is completed in accordance with the details set out in Annex IB of the Appendix of the EU SCC.

c. For the purposes of Clause 4 (Responsibilities of the Parties) of the Brazilian SCC, where Client acts as a Controller of Client Personal Data, it shall be the Designated Party (as defined in the Brazilian SCC) for the purposes of Clause 14 (Transparency), Clause 15 (Data Subject Rights), and Clause 16 (Incident Reporting). In cases where Client acts as a Processor on behalf of other Controllers, option B applies and the relevant Third-Party Controller (as defined in the Brazilian SCC) is identified based on the information provided pursuant to Section 1.1. of the DPA.

d. Information required to complete Section 3 (Security Measures) of the Brazilian SCC is set forth in the Annex II of the Appendix of the EU SCC.

2. The Country Required Terms (CRT)

Depending on the applicable Data Protection Laws, the parties can be subject to additional country required terms. The CRT contains a list of country unique requirements applying to Client and IBM, in accordance with the applicable Data Protection Laws. Only the relevant section of the CRT will apply to Client and IBM, in accordance with the Agreement and the applicable Data Protection Laws.

2.1 De-identified Data provisions under California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (CCPA), Virginia Consumer Data Protection Act (VCDPA) and any Data Protection Laws having similar requirements.

IBM will Process any de-identified data provided by Client, as defined by VCDPA, CCPA and any Data Protection Laws having similar requirements (De-identified Data), without attempting to re-identify it. IBM will take reasonable measures that are available to IBM to avoid De-Identified Data being associated with a Data Subject. If IBM is instructed by Client in a TD to re-identify De-identified Data, IBM will treat De-identified Data as Client Personal Data subject to the terms of the DPA.

2.2 Specific Personal Information provisions under the Japanese My Number Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No.27 of 2013).

Client acknowledges that IBM's Service is not designed to handle Specific Personal Information as defined and subject to the Japanese My Number Act (i.e., the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No.27 of 2013), as may be amended), unless otherwise agreed between IBM and Client in the Agreement.