Change information:
- December 2021: Singapore Personal Data Protection Act (PDPA) added
- November 2021: China Personal Information Protection Law (PIPL) added.
- September 2021: UK Data Protection reference updated
- March 2021: UK Data Protection Act 2018 reference updated.
- December 2020: Appendix on Additional Safeguards to EU Standard Contractual Clauses (EU SCCs).
- July 2020: Brazil's General Data Protection Law, Lei Geral de Proteção de Dados (LGPD) data protection law updated.
- July 2020: Serbia Data Protection Law updated.
- March 2020: Brazil's General Data Protection Law, Lei Geral de Proteção de Dados (LGPD) data protection law added.
- March 2020: UK Data Protection Act 2018 added to United Kingdom.
- December 2019: California Consumer Privacy Act of 2018 data protection law added.
- September 2019: European Economic Area data protection law added.
- August 2019: Serbia data protection law added.

The IBM Data Processing Addendum at http://www.ibm.com/dpa (DPA) applies to the Processing of Personal Data by IBM on behalf of Client under the Agreement in order to provide and improve the IBM Services and other IBM services that utilize the same underlying technology or tools, and as otherwise set out in the Agreement, if and to the extent i) the European General Data Protection Regulation (EU/2016/679) (GDPR); or ii) any other data protection laws identified below apply.

The Appendix on Additional Safeguards to EU Standard Contractual Clauses, reported below, supplements and is made part of the EU SCCs, set out in the DPA Exhibit, as applicable.

The DPA prevails over any conflicting term of the Agreement.

European Economic Area:
European Union Regulations and EEA Member State laws, other than GDPR, requiring a contract governing the processing of personal data, identical to or substantially similar to the requirements specified in Art. 28 of the GDPR.

United Kingdom:
The UK General Data Protection Regulation (as incorporated into UK law under the European Union (Withdrawal) Act 2018), and the UK Data Protection Act 2018, both as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, as amended, superseded or replaced.

For the purpose of Section 8 of the DPA, the European Commission decision 2010/87/EU on standard contractual clauses will be implemented for transfers to Non-Adequate Countries subject to the UK General Data Protection Regulation (UK SCC).

By entering into the Agreement, Client is entering into UK SCC with each IBM affiliate (IBM Companies) that has signed the UK SCC found at:

for IBM Technical Support Services: http://ibm.com/terms?id=tss-euscc&cc=uk
for IBM Managed Security Services: http://ibm.com/terms?id=security_services-idp_managed&cc=uk
for IBM Cloud & Lab Services: http://ibm.com/terms?id=SW-EUSSC&cc=uk

for all other IBM Services: attached to the DPA Exhibit

IBM or an IBM Companies shall enter into back-to-back UK SCC in accordance with Clause 11 of the UK SCC with any a Subprocessor listed in the DPA Exhibit that is located in a Non-Adequate Country and is not an IBM Data Importer.

Serbia:
Law on Personal Data Protection (Zakon o zaštiti podataka o ličnosti; Official Gazette of the Republic of Serbia, no 87/2018).
In the case of a transfer of Client Personal Data to a Non-Adequate Country, by entering into the Agreement, the Client is entering to the Serbian Standard Contractual Clauses (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. References to the EU Standard Contractual Clauses (EU SCC) in Section 8 of the DPA and in the DPA Exhibit shall mean the Serbian SCC.

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.

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.

Brazil:
The Brazil's General Data Protection Law, Lei Geral de Proteção de Dados (LGPD), upon entering into force. For the sake of clarity, IBM's obligations to a Client under the DPA are only those express obligations imposed by LGPD on a "Data Processor (operador)" for the benefit of a "Data Controller (Controlador)" (including new Section 1.6 below), as "Data Controller (controlador)" and "Data Processor (operador)" are defined by the LGPD:

1.6 Each party is responsible to fulfil its respective obligations set out in the LGPD, and Client will only issue Processing instructions, as set forth in Section 1.3 of this DPA, that enable IBM to fulfill its LGPD obligations.
For the purpose of Section 8, the EU SCC will be used for transfers to non-adequate countries as per GDPR.

State of California, United States:
The California Consumer Privacy Act of 2018 (CCPA) upon entering into force. IBM's obligations to Client under the DPA are those that the CCPA requires that a "Business" have in place with a "Service Provider" (including new Section 1.6 below), as "Service Provider" and "Business" are defined by the CCPA:

> **1.6** IBM will not further collect, sell, retain, disclose or use the Personal Information of the Consumer for any purpose other than to perform the Services specified in the Agreement, or as otherwise permitted by CCPA. IBM certifies that it understands and will comply with the restrictions set forth in this Section 1.6.
> The terms used in the applicable provisions of the DPA shall be replaced as follows:
> "Personal Data" shall mean "Personal Information"; "Controller" shall mean "Business"; "Processor" shall mean "Service Provider"; and "Data Subject" shall mean "Consumer".

China:
The People's Republic of China Personal Information Protection Law (PIPL) upon entering into force. For the sake of clarity, IBM's obligations to Client under the DPA are those that the PIPL requires that IBM as "Entrusted Person" have in place with a "Personal Information Handler, as "Entrusted Person" and "Personal Information Handler" are referenced in the PIPL.

Singapore:
The Personal Data Protection Act 2012 No. 26 of 2012, as amended from time to time, and its accompanying regulations. For the sake of clarity, IBM's obligations to Client under the DPA are only those express obligations imposed by PDPA on a "Data Processor (data intermediary)" when processing personal data on behalf of "Data Controller (organisation)" pursuant to a contract, as "organisation" and "data intermediary" are defined by the PDPA.

In case of a transfer of Client Personal Data outside of Singapore, the DPA applies excluding Section 8.

Appendix on Additional Safeguards to EU Standard Contractual Clauses (EU SCCs)
1. 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 European Union (EU) Standard Contractual Clauses (SCCs) to those countries whose laws are likely to have a substantial adverse effect on the level of data protection offered by the EU SCCs and required under EU data protection law.
2. IBM will implement and maintain the technical and organizational measures, as specified in the 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 the IBM's scope of responsibility.

3. 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").
4. In the event of any such request for access to Client Personal Data by a government or regulatory authority:
    a. in accordance with the Data Access Letter and Transparency Report, IBM will notify Client of such request to enable the Client to take all necessary actions to communicate directly with the relevant authority and respond to such request. If IBM is prohibited by law to notify the 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; and
    b. if, regardless of all such efforts, IBM is prohibited by law to notify the Client, upon request of the Client and in accordance with applicable law, IBM will provide to such Client general information relative to any such request received from a government or regulatory authority during the preceding 12-month period.

DPA-DPL-11_12-2021_zz-en