IBM Managed Security Services

This Data Processing Addendum Exhibit (DPA Exhibit) specifies the DPA for the identified Service.

1.   Processing

IBM will process Client Personal Data for the Service, as described in the Service Description and as supplemented and specified by this DPA Exhibit.

1.1   Duration of Processing

The duration of the Processing will be for the period of the contract term as listed within the Transaction Document (TD).

1.2   Processing Activities

The processing activities with regard to Client Personal Data are specified in the SOW and may include:

- Receipt of Client Personal Data from Client and/or other third parties
- Computer processing of Personal Data, including data transmission, data retrieval, data access, and network access to allow data transfer if required
- Technical testing of computing environments when this testing results in access to Client Personal Data
- Monitoring of computing environments for security threats when this monitoring results in access to Client Personal Data
- Technical customer support
- Transformation and transition of Client Personal Data as necessary to deliver the Services

2.   Client Personal Data

2.1   Categories of Data Subjects

The following list indicates the typical types of Personal Data that may be processed by IBM as a part of the Services and as specified in the SOW:

- Data Subjects associated with Client Personal Data that are processed as part of the Service include Client employees, customers, business partners, and suppliers.

Given the nature of the Services, Client acknowledges that IBM is not able to verify or maintain the above list of Categories of Data Subjects. Therefore, Client will notify IBM about any required changes of the list above by updating the related Statement of Work (SOW) via the established Project Change Request (PCR). IBM will process Personal Data of all Data Subjects listed above in accordance with the Agreement. If changes to the list of Categories of Data Subjects require changes of the agreed Processing, Client shall provide Additional Instructions to IBM as set out in the DPA.

2.2   Types of Client Personal Data and Special Categories of Client Personal Data

The Personal Data processed concern the following categories of Personal Data:

Log files and event data transferred from the Client to IBM, in order to deliver the contracted security and compliance services.

The following list sets out what Types of Client Personal Data may be processed within the Services. Any deviations to the following list to be processed will be explicitly stated within the related SOW.

- Business Contact Information
  - *(e.g., name, address, phone number, email, etc.)*
- Technically Identifiable Personal Data

- *(e.g., device IDs, usage based identifiers, static IP addresses, all when linked to an individual)*
- Employment-Related Personal Data
  - *(e.g., any HR data, including job history, performance review information, etc.)*
- Location Information
  - *(e.g., geolocation data associated with an individual)*

2.2.1 Special Categories of Personal Data

No Special Categories of Personal Data will be provided to IBM by the Client unless specifically provided in writing (such Special Categories of Personal Data including, but not limited to, personal information related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, or biometric data). In the case that Special Categories of Personal Data are included for Processing, the Client will notify IBM of the data type(s) in question, in writing by amendment to the SOW. IBM will confirm the data types and assess any subsequent impact on the provision of the Services via the established Project Change Control (PCR) process and the specific data type(s) will be explicitly stated within the related SOW.

2.2.2 General

The lists set out in sections 2.2.1 and 2.2.2 above are information about the Types of Client Personal Data and Special Categories of Client Personal Data generally can be processed within the Services. Given the nature of the Services, Client acknowledges that IBM is not able to verify or maintain the above lists of Types of Client Personal Data and Special Categories of Client Personal Data. Therefore, Client will notify IBM about any required changes of the lists above by updating the related SOW via the established Project Change Request (PCR) process.

IBM will process all Types of Client Personal Data and Special Categories of Client Personal Data listed above in accordance with the Agreement. If changes to the lists of Types of Client Personal Data and Special Categories of Client Personal Data require changes of the agreed Processing, Client shall provide Additional Instructions to IBM as set out in the DPA.

3. Technical and Organizational Measures

The Technical and Organizational Measures ("TOMs") published at https://www.ibm.com/services/us/tom/ apply to all Client Personal Data. These TOMs as set out above are applicable to Client Personal Data as described in section 2 above or as otherwise included within the Service Description.

Client confirms its obligation to implement appropriate TOMs within its own area of responsibility as required by applicable Data Protection Laws.

Upon request from the Client, evidence of the implementation of measures may be presented in the form of:

- Up-to-date attestations, reports or extracts thereof from independent bodies (for example: external auditors, internal audit, the data protection officer, the IT security department or quality auditors)
- Suitable certification by way of an IT security or data protection audit
- European Commission approved data protection certification mechanisms, seals or marks
- Responses on specific questions from the Client which are highlighted by the customer as not covered in the above

4. Deletion and Return of Client Personal Data

IBM will delete Client Personal Data at the end of the Services. However, if instructed in writing prior to such expiration or termination of the Services, IBM will return a copy of Client Personal Data that is accessible to IBM within a reasonable period and in a reasonable format at Client's expense according to the terms for Assistance as set forth in the DPA.

If applicable for the Service, Client is responsible to securely erase all data (including confidential, proprietary and Client Personal Data) from any Machine or part of a Machine returned to IBM for any reason and ensure that it is free of any legal restrictions that would prevent its return. Client may purchase an offering for retention or purchase an offering to have IBM delete or destroy the Client Personal Data.

5. Subprocessors

IBM may use the following Subprocessor(s) (Security Operations Centers ("SOCs") and MSS subprocessors) in the Processing of Client Personal Data for the respective Service: https://www-03.ibm.com/security/services/managed-security-services/security-operations-centers.html

This agreed list of sub-processors may be amended or altered from time to time, in writing, by the Parties, in accordance with the established PCR process as outlined in the SOW.

IBM will notify Client of any intended changes to Sub-processors as follows:

- Publishing changes the website listed within this section;
- A notification to registered users of the Global SOC Portal.

6. International Data Transfer

6.1 EU-U.S. and Swiss-U.S. Privacy Shield self-certification

IBM Global Managed Security Services ("MSS") has self-certified with Privacy Shield as published on https://www.privacyshield.gov/participant?id=a2zt0000000TOAoAAO and further detailed with a list of certified IBM Services on https://www.ibm.com/privacy/details/us/en/privacy_shield.html.

Based on the Privacy Shield onwards transfer principle, Personal Data is transferred onwards by MSS US as the main processor to the Sub-processors listed in Section 5. Sub-processor agreements have been executed between MSS US as the main-processor and the remaining Sub-processors, stating that the same level of protection is provided.

6.2 EU Standard Contractual Clauses

For global MSS services involving service delivery from non-EEA Security Operations Centers (SOCs), the EU Standard Contractual Clauses signed by or on behalf of all IBM Data Importers if applicable for the Service, are available at: https://www.ibm.com/services/us/dpa/.

7. Data Privacy Officer and Other Controllers

Client is responsible for providing complete, accurate and up-to-date information about its data privacy officer and each other Controllers (including their data privacy officer). Any updates to the information should be provided to IBM by contacting DPA.Help.project@uk.ibm.com along with the contract # and client name.

8. IBM Privacy Contact

The IBM privacy contact can be contacted at DPA.Help.project@uk.ibm.com.