IBM Data Processing Addendum (with EU Standard Contractual Clauses)

(Final Version November 2016)

This Addendum is part of the Agreement for the Cloud Services between Client and the respective IBM company (IBM Contracting Party). The parties to this Addendum are (1) Client on its own behalf and on behalf of controllers (including its affiliates and third parties) that Client authorizes to use the Cloud Services, and (2) the IBM Contracting Party and the IBM companies listed in Exhibit 2 as data processors that may be used by the IBM Contracting Party to process the Client Personal Data for the purpose of providing the Cloud Services (collectively, IBM Data Processors). This Addendum has two parts: (1) the data processing terms including Exhibit 2 which apply to all IBM Data Processors; and (2) the standard contractual clauses for the transfer of personal data to processors established in third countries (Commission Decision 2010/87/EC) with optional clauses removed, attached to this Addendum as Exhibit 1 (EU Standard Contractual Clauses) which apply only to the IBM Data Processors that are established outside the European Economic Area and countries considered by the European Commission to have adequate protections as listed in table 2 of Exhibit 2.

1. Processing

1.1 If Client includes, or authorizes others to include, personal data in the content input into the Cloud Services or personal data is generated in performance of the Cloud Services (Client Personal Data), Client represents that it is either the data controller of the Client Personal Data or that it has, prior to agreeing to the provisions of this Addendum or extending the benefit of the Cloud Services to any new data controller, been instructed by or obtained the consent of the relevant data controller(s) to agree to the undertakings in this Addendum. Client appoints IBM Data Processors as data processors to process (as those terms are defined in EU Directive 95/46/EC, as amended or replaced, from time to time) such Client Personal Data. Client and IBM Contracting Party agree (and will procure that the data controllers and IBM Data Processors agree) that any disputes or liability under this Addendum will be subject to the limitation and exclusions of liability in the Agreement.

1.2 The purpose of the processing of the Client Personal Data by IBM Data Processors on behalf of Client is to provide the Cloud Services, and the subject matter, duration, and purpose are further described in the Transaction Documents and Attachments to the Agreement. The categories of data subjects, types of Client Personal Data, and processing operations and nature of processing are set out below:

Categories of Data Subjects

Unless instructed otherwise by Client, data subjects may include Client's and its affiliates' employees, contractors, business partners, other individuals, and to the extent required by law legal entities whose personal data is processed by the Cloud Services.

Types of Client Personal Data

The Client Personal Data transferred concern the following types of data:

Client determines the types of data per each Cloud Service subscribed. Client's data fields can be configured as part of the implementation of the Cloud Service or as otherwise permitted in the Cloud Service. Identified representatives of Client determine what Client Personal Data is processed based on their business processes and corresponding use of the Cloud Service. The personal data processed across all Cloud Services usually concern (a subset of) the following categories of data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, and to the extent applicable legal entity information.

Processing operations and nature of processing

The Client Personal Data processed by IBM Data Processors will be subject to the following basic processing activities:

- use of Client Personal Data to provide the Cloud Services and to provide assistance to technical support
- storage of Client Personal Data in data centers
- back up of Client Personal Data
- computer processing of Client Personal Data, including data transmission, data retrieval, data access

- network access to allow Client Personal Data transfer, if required

1.3 Except as otherwise set out in the Agreement, the IBM Data Processors will only process Client Personal Data for the purpose of providing the Cloud Services in accordance with this Agreement. Client and IBM Data Processors shall take steps to ensure that any person acting under their authority who has access to the Client Personal Data shall not process such Client Personal Data for any other purposes, unless required to do so by applicable law.

1.4 IBM Data Processors will process Client Personal Data according to Client's instructions. Client's complete and final instructions for the processing of Client Personal Data are defined by the purposes set out in Sections 1.2 and 1.3 above and this Agreement as well as Client's and its authorized users' use and configuration of features in the Cloud Service. If an additional instruction is necessary to meet mandatory legal requirements and the IBM Contracting Party is not able to accommodate the requested changes, then Client may terminate the Cloud Service by providing the IBM Contracting Party with written notice. IBM will refund any prepaid charges prorated from the termination date. Instructions given by Client have to be addressed to IBM Contracting Party and may include the correction, deletion, or blocking of Client Personal Data where the Cloud Service does not already enable Client to do so itself. Without prejudice to Client's obligations as the sole controller, if IBM Contracting Party believes Client´s instruction could be violating data privacy provisions, IBM Contracting Party will inform Client without undue delay. IBM Contracting Party will be entitled to suspend the performance of the relevant instruction until Client has confirmed or modified the instruction accordingly. Client will immediately declare the confirmation or modification in writing.

1.5 Client shall enter into data processing agreements with other controllers in order to allow IBM Data Processors as processors and their subprocessors to process any Client Personal Data. Client shall serve as a single point of contact for the IBM Contracting Party and is solely responsible for the internal coordination, review, and submission of instructions or requests of other controllers to the IBM Contracting Party. The IBM Contracting Party shall be discharged of its obligation to inform or notify a controller when it has provided such information or notice to Client. The IBM Contracting Party is entitled to refuse any instructions provided directly by a controller that is not Client. Similarly, the IBM Contracting Party will serve as a single point of contact for Client and is solely responsible for the internal coordination, review, and submission of instructions or requests from Client to IBM Data Processors other than IBM Contracting Party as well as for obtaining, prior to having the Cloud Services launched, all necessary permissions and regulatory approvals for such processing. If for any reason this Addendum is held to be invalid with respect to any controllers other than Client, any use of the Cloud Services by such other controllers shall be deemed authorized by Client, in the name and on behalf of Client.

1.6 IBM Data Processors will comply with all data protection laws and regulations in respect of the Cloud Services applicable to data processors. IBM Contracting Party is not responsible for determining the requirements of laws applicable to Client's business or that IBM Contracting Party's provision of the Cloud Services meets the requirements of such laws. Client will not use the Cloud Services in conjunction with personal data to the extent that doing so would violate applicable data protection laws. Client will be solely responsible for the lawfulness of the agreed data processing by IBM Contracting Party, in particular for the lawfulness of the transmission of Client Personal Data to IBM Data Processors. Client confirms that it has taken into consideration professional, technical, organizational, and personal competences of the IBM Data Processors and their capability to ensure security of processed Client Personal Data when the Cloud Service was selected by Client.

2. Technical and organizational measures

2.1 IBM Data Processors will implement and maintain, or may enable Client to implement and maintain as described in the applicable Transaction Documents or Attachment, the following practices and procedures, which may be revised periodically, regarding the systems used to host and operate the Cloud Services:

1. Security Policies

Information security policies of the IBM group of companies (IBM) are reviewed at least annually and refined as necessary to keep current with modern threats and in line with updates to broadly accepted international standards, such as ISO/IEC 27001 and 27002.

IBM follows a mandated set of employment verification requirements for all new hires, including supplemental employees. These standards also apply to wholly owned subsidiaries and joint ventures. The requirements, which may be subject to change, include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks if the candidate previously worked for a government entity. Each IBM Data Processor is responsible for implementing the above requirements in its hiring process as applicable and permissible under local law.

IBM employees are required to complete security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security requirements, as set out in IBM's Business Conduct Guidelines.

Security incidents are handled in accordance with IBM incident management and response policies, taking into account data breach notification requirements under applicable law.

The core functions of IBM's global cybersecurity incident management practice are conducted by IBM's Computer Security Incident Response Team (CSIRT). CSIRT is managed by IBM's Chief Information Security Office and is staffed with global incident managers and forensic analysts. National Institute of Standards and Technology, United States Department of Commerce (NIST) guidelines for computer security incident handling have informed the development and remain the foundation of IBM's global incident management processes.

CSIRT coordinates with other functions within IBM to investigate suspected incidents, and if warranted, define and execute the appropriate response plan. Upon determining that a security incident has occurred that affects Client, IBM Contracting Party will notify Client, as appropriate.

2. Access, Intervention, Transfer and Separation Control

The architecture of the Cloud Services maintains logical separation of Client Personal Data. Internal rules and measures separate data processing, such as reading, inserting, copying, amending, making available, deleting, and transferring Client Personal Data, according to the contracted purposes. Access to Client's data, including any Client Personal Data, is allowed only by authorized personnel in accordance with principles of segregation of duties, strictly controlled under identity and access management policies, and monitored in accordance with IBM's internal privileged user monitoring and auditing program.

IBM's privileged access authorization is individual, role-based, and subject to regular validation. Access to Client Personal Data is restricted to the level required to deliver services and support to Client (i.e., least required privilege).

Transfer of Client Personal Data within IBM's network takes place on wired infrastructure and behind firewalls, without the use of wireless networking.

Upon expiration or cancellation of the Cloud Services, Client Personal Data is rendered unrecoverable in conformity with NIST guidelines for media sanitization, or earlier upon Client's request.

3. Service Integrity & Availability Controls

The Cloud Services undergo penetration testing and vulnerability scanning prior to production release. Additionally, penetration testing, vulnerability scanning, and ethical hacking is performed regularly by IBM and authorized independent third parties.

Modifications to operating system resources and application software are governed by IBM change management policies. Changes to network devices and firewall rules are also governed by the change management policies and are separately assessed for security risk prior to implementation.

IBM's data center services support a variety of information delivery protocols for transmission of data over public networks, such as HTTPS, SFTP, and FTPS. IBM systematically monitors production data center

resources 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators to help detect and resolve potential exposures.

The Cloud Services have business continuity and disaster recovery plans, which are developed, maintained, verified, and tested in compliance with the ISO 27002 Code of Practice for Information Security Controls. Recovery point and time objectives for the Cloud Services are established according to their architecture and intended use and provided in the applicable TD or Attachment. Backup data intended for off-site storage, if any, is encrypted prior to transport.

Security configuration and patch management activities are performed and reviewed regularly. IBM's infrastructure is subject to emergency planning concepts, such as disaster recovery and solid disk mirroring. Business continuity plans for IBM's infrastructure are documented and regularly revalidated.

4. Activity Logging, Input Control

IBM policy requires administrative access and activity in the Cloud Services' computing environments to be logged and monitored, and the logs to be archived and retained in compliance with IBM's worldwide records management plan. Changes made to production Cloud Services are recorded and managed in compliance with IBM change management policy.

5. Physical Security, Entry Control

IBM maintains physical security standards designed to restrict unauthorized physical access to data center resources. Entry points into IBM data centers are limited, controlled by access readers, and monitored by surveillance cameras. Access is allowed only by authorized personnel.

Delivery areas and loading docks where unauthorized persons may enter the premises are strictly controlled. Deliveries are scheduled in advance and require approval by authorized personnel. Personnel who are not part of the operations, facilities, or security staff are registered upon entering the premises and are escorted by authorized personnel while on the premises.

Upon termination of employment, employees are removed from the access list and required to surrender their access badges. Use of access badges is logged.

6. Order Control

Data processing is performed only according to Client's instructions. Client's complete and final instructions for the processing of Client Personal Data are defined by Client's and its authorized users' use and configuration of the features in the Cloud Service and the purpose set out in Section 1.2 above and the Agreement, which describes the terms, functionality, support, and maintenance of a Cloud Service and measures taken to ensure the confidentiality, integrity, and availability of Client Personal Data.

7. Compliance

IBM information security standards and management practices for Cloud Services are aligned to the ISO/IEC 27001 standard for information security management and comply with the ISO/IEC 27002 Code of Practice for Information Security Controls. Assessments and audits are conducted regularly by IBM to track compliance with its information security standards. Additionally, independent third party industry standard audits are performed annually in all IBM production data centers.

2.2. The IBM Data Processors shall implement appropriate technical and organizational security measures as required by applicable mandatory law, which measures are incorporated by reference.

2.3 IBM security measures are subject to technical progress and further development. Accordingly, IBM Contracting Party reserves the right to modify the IBM security measures provided that the functionality and security of the Cloud Services are not degraded. Additional measures requested by Client will be in accordance with Section 1.4 above.

2.4 Client (1) confirms that the above measures provide an adequate level of protection for the Client Personal Data, and (2) will ensures that only personal data strictly required for the Cloud Service is included in the Client Personal Data.

3. Access

3.1 To the extent permitted by law, IBM Contracting Party will inform Client without delay of data subjects' requests for rectification, deletion, blocking of data, and enforcement of privacy rights in accordance with applicable law, complaints from data subjects, and/or objections from competent regulators. Upon notification by IBM Contracting Party, Client is responsible for handling such data subjects' requests. If Client is obliged to provide information regarding Client Personal Data to third parties (including data subjects or competent regulators), IBM will support Client to a reasonable extent, provided that (1) Client has requested IBM Contracting Party in writing and (2) Client agrees to pay the cost of any support (including internal resources) provided by IBM Contracting Party or its subcontractors (including the IBM Data Processors) based on the rates set out in IBM's price list for consulting services in excess of four hours per year.

3.2 IBM Contracting Party and IBM Data Processors will not disclose Client content to any unauthorized third party subject to mandatory law. If a government demands access to Client Personal Data, IBM Contracting Party will notify Client prior to disclosure unless prohibited by law.

3.3 IBM Contracting Party and IBM Data Processors require all personnel authorized to process Client Personal Data to commit themselves to confidentiality and complete annual security and privacy training. Such an obligation of confidentiality shall continue to be valid after termination of the Agreement and/or of their activity.

3.4 Client and IBM Contracting Party will inform each other without delay of any suspected non-compliance with applicable data protection laws and regulations or relevant contractual terms. Client and IBM Contracting Party will support each other in order to rectify any non-compliance as soon as reasonably practicable.

4. Audit

4.1 IBM Data Processors have obtained the standard security certifications and personal data seals and marks listed at the following Web pages for IBM SaaS http://www.ibm.com/cloud-computing/built-on-cloud/saas-security and for IBM Bluemix https://www.ibm.com/cloud-computing/bluemix/trust-security-privacy.

4.2 Upon Client's written request, IBM Contracting Party will provide Client with the most recent certifications and/or summary audit report(s) concerning the security measures for the Cloud Service or IBM computing environment used to provide the Cloud Service. IBM Contracting Party will reasonably cooperate with Client by providing available additional information to help Client better understand such security measures. To the extent it is not possible to otherwise satisfy an audit obligation mandated by applicable law, only the legally mandated entity (such as a governmental regulatory agency having oversight of Client's operations) or legally mandated functions within such entity (such as the internal controls function) may conduct an onsite visit of the facilities used to provide the Cloud Service, and only in a manner that causes minimal disruption to IBM's business and in accordance with IBM's security policies to reduce any risk to IBM's other customers. Unless mandated by law, no audits are allowed within a data center for security and compliance reasons. Client agrees to pay the costs of any support provided by IBM (including internal resources) based on the rates set out in IBM Contracting Party's price list for consulting services in excess of four hours per year.

4.3 To the extent permitted by applicable law, Client agrees to exercise its audit right (as set out above and, if applicable, in Clause 5 (f) of the EU Standard Contractual Clauses) by instructing IBM Data Processors to execute the audit as described in this Section 4. Changes of this instruction have to be in writing.

4.4 The IBM Data Processor obligations stated above in Section 4.3 and, as applicable, in Clause 12 paragraph 2 of the EU Standard Contractual Clauses shall be replaced and superseded in their entirety by the IBM Data Processors obtaining a personal data protection seal or mark, or by the adherence to a certification mechanism or a code of conduct, considered by the European Data Protection Board or the European supervisory authorities as an element to demonstrate sufficient guarantees of appropriate safeguards.

5. IBM Privacy Contact

5. 1 The IBM privacy contact for the European Economic Area and Switzerland can be contacted at eu-mc@ie.ibm.com.

6. Return or Deletion of Client Personal Data

6.1 Unless otherwise required by applicable law, IBM Contracting Party will destroy the Client Personal Data upon termination or expiration of a Cloud Service within a reasonable period. However, IBM will return the Client Personal Data within a reasonable period in a reasonable and common format upon receiving written instructions from the Client prior to termination or expiration, provided that the Client Personal Data is available to IBM. IBM Contracting Party shall have no obligation to return Client Personal Data to Client if the Client Personal Data is available to Client or the other data controllers.

7. IBM Data Processors and Subprocessors

7.1 Client agrees that IBM Contracting Party may use the other IBM Data Processors to process the Client Personal Data in accordance with the Agreement. Client agrees that IBM Data Processors are entitled to engage subprocessors. A list of the countries where Client Personal Data may be processed is available at www.ibm.com/cloud/datacenters or as described in the applicable Transaction Documents or Attachment to the Agreement. A list of subprocessors including their addresses is available upon request. When engaging subprocessors IBM Data Processors shall conclude agreements with the subprocessors to bind them to obligations which are essentially the same as those set out in this Addendum. To the extent required, Client explicitly mandates IBM Data Processors to sign these agreements directly with the subprocessors. Client will only contact the IBM Data Processors or subprocessors in coordination with IBM Contracting Party.

7.2 IBM Contracting Party will notify Client in advance of any changes to IBM Data Processors or subprocessors using regular communication means such as client newsletters, websites, and portals. IBM will procure that any new data processor that is an IBM company will accede to this Addendum as new IBM Data Processor. The parties to this Addendum declare in advance that they accept such additional IBM Data Processor as a party under this Addendum and accept to be bound thereto. If Client reasonably objects to the addition of a new data processor or subprocessor (e.g., such change causes Client to be non-compliant with applicable data protection laws), Client shall notify IBM Contracting Party in writing of its specific objections within 30 days of receiving such notification. If Client does not object within such period or objects but does not terminate the Cloud Service, the addition of the new subprocessor or data processor and, if applicable, the accession to this Addendum shall be considered accepted. If Client does object to the addition of a new data processor or subprocessor and IBM cannot accommodate Client's objection, Client may terminate the Cloud Service in writing within 60 days of receiving IBM's notification. For the avoidance of doubt, the IBM Contracting Party will not allow the new subprocessor or data processor to process Client Personal Data until the subprocessor or data processor is accepted by Client or the Cloud Service is terminated in accordance with this Section 7.2.

8. Transborder Data Processing

8.1 If IBM Data Processors are located outside of the European Economic Area or countries considered by the European Commission to have adequate protections (Data Importers), Client and Data Importers agree that by signing this Addendum they have entered into the EU Standard Contractual Clauses. Client will procure that each controller will accede to the EU Standard Contractual Clauses. In the event of a conflict between this Addendum and the EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall prevail. If required by relevant data protection authorities, IBM Contracting Party will cause Data Importers to enter into a separate, stand-alone Standard Contractual Clauses agreement with Client. If Client is a data processor in respect of the Client Personal Data, then Client will procure that the data controller(s) in respect of the Client Personal Data will enter into a separate data transfer agreement (including the EU Standard Contractual Clauses) available from eu-mc@ie.ibm.com.

9. Security Incidents

9.1 IBM Contracting Party will notify Client without undue delay after becoming aware of a breach of security in respect of the Cloud Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Personal Data transmitted, stored, or otherwise processed by any IBM Data Processor ("Personal Data Breach"). IBM Contracting Party will promptly investigate the Personal Data

Breach if it occurred on IBM IT infrastructure and will assist Client upon request by providing relevant information that Client requires to meet its mandatory legal obligations (including obligations to notify supervisory authorities or data subjects), if any, in relation to the Personal Data Breach, taking into account the nature of the processing and the information available to the IBM Contracting Party. IBM Contracting Party shall have no obligation to provide such information to Client in the event such information is available to Client from sources other than IBM.

10. Applicable Law and Forum, Duration

10.1 Without prejudice to Clause 9 and the rights of the data subjects and national supervisory authorities under the EU Standard Contractual Clauses, Client and IBM Data Processors agree that (1) governing law of this Addendum, and (2) the forum for all disputes in respect of this Addendum, shall be the same as set out in the Agreement, unless otherwise required by applicable law.

10.2 If the EU Standard Contractual Clauses apply, nothing in this Addendum varies or modifies the EU Standard Contractual Clauses or affects any supervisory authority's or data subject's rights under the EU Standard Contractual Clauses.

10.3 This Addendum shall have an indefinite duration except that the main body shall be valid until 24 May 2018 after which date it shall cease to apply.

11. Country Required Terms

11.1 For transactions performed in the countries specified below, the following terms replace or modify the referenced terms in this Addendum. All terms in this Addendum that are not changed by these amendments remain unchanged and in effect.

11.2 Mandatory Security Measures

In respect of controllers established in the following countries, the reference to appropriate technical and organizational security measures required by applicable law in Section 2.2 are replaced by:

a. in **Croatia**: Croatian Personal Data Protection Act - Article 10 (3);

b. in **Czech Republic**: Act. No. 101/2000 Coll. on Protection of Personal Data, as further amended;

c. in **Denmark**: If Client is a data controller subject to the Danish Act on Processing of Personal Data, the rules of the Executive Order on Security also apply to the processing by the IBM Data Processors. Further, any IBM Data Processor established in a different EEA Member State than Denmark is subject to the provisions on security measures laid down by law in the EEA Member State in which the IBM Data Processor is established;

d. in **Italy**: Annex B to D.Lgs. 196/2003;

e. in **Latvia**: Republic of Latvia Cabinet of Ministers Regulations No.40 of 30 January 2001 "Mandatory Technical and Organizational Requirements for Protection of Personal Data Processing";

f. in **Lithuania**: General Requirements for Organisational and Technical Data Security Means approved by Order No. 1T-74(1.12.E) of 18 December 2013 of the Director of the Inspectorate;

g. in **Poland**: Act of the Polish Parliament from August 29, 1997 on the Protection of Personal Data and the regulation of April 29, 2004 by the Minister of Internal Affairs and Administration as regards personal data processing documentation and technical and organisational conditions which should be fulfilled by devices and computer systems used for the personal data processing;

h. in **Slovakia**: Act No. 122/2013 Coll. On Protection of Personal Data, as further amended;

i. in **Spain**: Title VIII of the Spanish Royal Decree 1720/2007, which approves the regulation implementing the Organic Law 15/1999 on the protection of personal data; and

j. in **Switzerland**: Ordinance to the Federal Act on Data Protection of 14 June 1993.

11.3 In respect of data controllers established in **Italy**, the Client appoints the IBM Contracting Party as System Administrator (and explicitly mandates the IBM Contracting Party to appoint the IBM Data Processors as System Administrators), where the Cloud Service involves activities relating to system administrators, in accordance with the requirements of the General Provision of the Data Protection Authority of 27 November

2008 "Measures and provisions laid down for Data Controllers in respect of data processed using electronic means in connection with the attribution of functions of system administrator" as modified by Provision 25 June 2009 (Provisions), and in respect of this appointment the IBM Contracting Party (and the IBM Data Processors, if any) undertakes to comply with the following requirements:

1. to identify on an individual basis the employees acting as System Administrators with reference to the contract, with an analytic listing of the operational areas permitted on the basis of the authorization profile assigned, with reference to the Cloud Service;
2. to carefully assess the subjective characteristics of the individual (such as assessing the experience, skills and reliability) to whom it is intended to grant the title of System Administrator, with reference to the Cloud Service;
3. to make available to the Data Protection Authority, where necessary, or to the controller at the request of the latter, the information required to identify those individuals acting as "*system administrators*", including a list of the functions committed to them with reference to the Cloud Service;
4. to prepare a plan for verification of the work of System Administrators (at least yearly), with reference to the Cloud Service, in order to ensure monitoring the extent to which their work complies with the measures contained in the Provisions;
5. where the systems and/or archives are under IBM Contracting Party's (or IBM Data Processors') control to adopt systems suitable for the registration of logical access (IT authentication) - for a period not shorter than 6 months - to processing systems and electronic archives by the System Administrators, with reference to the Cloud Service, which have the characteristics provided for by the Provisions in relation to completeness, immutability and possibility of verification of their integrity.

11.4 In respect of controllers established in **Cyprus** and **Greece**, respectively, Sections 2.1(6) and 2.4 are amended by adding the following phrase to the beginning of each Section: (1) "Subject to the IBM Data Processors' obligations under art. 10 of Law 138 (I) 2001 as amended from time to time and in force" for Cyprus, and (2) "Subject to the IBM Data Processors' obligations under art. 10 of Law 2472/1997 as amended from time to time and in force" for Greece.

11.5 In respect of controllers established in **Switzerland**, references to:

a. "EU Directive 95/46/EC" are replaced by "Federal Act on Data Protection (FADP) of 19 June 1992";

b. "EU Standard Contractual Clauses" are replaced by "Swiss Transborder Data Flow Agreement";

c. "Commission Decision 2010/87/EC" are replaced by "art. 6, para. 2, letter a. Federal Act on Data Protection"; and

d. "European Data Protection Board" or "European supervisory authorities" are replaced by "Federal Data Protection and Information Commissioner";

e. "European Commission" are replaced by "Federal Data Protection and Information Commissioner";

By signing below, Client acknowledges that it is executing this Addendum, including the EU Standard Contractual Clauses and all appendices, on its own behalf as a controller and on behalf of its affiliates or third parties as controllers which it has authorized to use the Cloud Services:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data processors listed in Exhibit 2 based on powers of attorney:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

EXHIBIT 1:
EU Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address:.....

Tel.: ..... ; fax:.....; e-mail: .....

Other information needed to identify the organisation:

.....

(the data **exporter**)

And

Name of the data importing organisation: .....

Address: .....

Tel.:.....; fax: ..... ; e-mail:.....

Other information needed to identify the organisation:

.....

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

The parties may provide further details in an offering agreement for the Cloud Services, if required.

Data exporter

The data exporter is an entity (the "Client") that has contracted with an affiliate of the data importers (the "IBM Contracting Party") for the Cloud Services which allows its authorized users to enter, amend, use, delete or otherwise process personal data. Client is entering into these Clauses on its own behalf as a controller and on behalf of its affiliates or third parties as controllers authorized by Client to use the Cloud Services.

Data importer

The data importers are affiliates of the IBM Contracting Party, which provide information technology services in respect to the Cloud Services.

Data subjects

The description of categories of data subjects as set out in Section 1.2 of the IBM Data Processor Addendum (including EU Standard Contractual Clauses) are incorporated into this Appendix 1 by reference.

Categories of data

The description of types of Client Personal data as set out in Section 1.2 of the IBM Data Processor Addendum (including EU Standard Contractual Clauses) are incorporated into this Appendix 1 by reference.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

As notified by Client in writing.

Processing operations

The nature (extent and type) of the processing as set out in Section 1.2 of the IBM Data Processor Addendum (including EU Standard Contractual Clauses) are incorporated into this Appendix 1 by reference.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organizational security measures set out in clause 2.1 of the IBM Data Processor Addendum (including EU Standard Contractual Clauses) are incorporated into this Appendix 2 by reference and are binding on the data importers. The data importers have implemented and will maintain these technical and organizational security measures for the purpose of protecting Client content against accidental loss, destruction, alteration, unauthorized disclosure or access, or unlawful destruction.

EXHIBIT 2:
IBM DATA PROCESSORS (INCLUDING DATA IMPORTERS)

To be provided separately