DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "DPA") is entered into as of the last date signed below (the "Effective Date") by and between Xcitium Inc., having an address of 200 Broadacres Drive, Second Floor, Bloomfield, NJ 07003, or an Xcitium Affiliate, (collectively hereafter the "Processor" or "Xcitium"), and customer identified below, on its behalf and in the name and on behalf of its affiliated companies (the "Controller"). This DPA may refer to Controller and Processor each as a "Party" and collectively as the "Parties." Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

1. INTRODUCTION

1.1. Controller has procured certain services provided by Processor pursuant to a written or electronic agreement ("Agreement"), attached hereto at the Agreement Appendix. This DPA satisfies Article 28 (3) of the GDPR (defined below) between Controller and Processor),and is incorporated in the Agreement and is intended to reflect the Parties' agreement with regard to the Processing of Personal Data.

1.2. Processor receives and/or is granted access to Personal Data (as defined below) in connection with the provision of the services under the Agreement.

1.3. To comply with applicable European Union Data Protection Legislation (including Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR") and laws implementing or supplementing the GDPR), Controller requires Processor to agree to this DPA. For the United Kingdom, the applicable laws are referenced as UK GDPR and DPA 2018.

1.4. Controller and Processor wish to agree to this DPA on the terms and conditions stated below.

1.5. The obligations and rights of Controller and Controller's affiliates (as applicable) are set out in the Agreement and the DPA.

2. DEFINITIONS

In addition to capitalized terms defined in the Agreement, the following terms shall bear the following meanings:

2.1 "**Applicable Law**" means any applicable (a) statute, regulation, regulatory requirement, by law, ordinance, subordinate legislation, or other law (regardless of its source), mandatory guidance, or code of practice (including in each case any judicial or administrative interpretation of it) in force from time to time in any applicable jurisdiction; or (b) judgment of a relevant court of law or sanction, directive, order, or requirement of any regulatory authority.

2.2 **"Xcitium Affiliate"** means an entity which is controlled by, controls or is in or under common control with Xcitium Inc. This includes Comodo Security Solutions, Ltd, located in the United Kingdom.

2.3 "**Data Protection Legislation**" means European Directives 95/46/EC and 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the GDPR), and all other applicable laws relating to the processing of Personal Data and privacy that may exist in any relevant jurisdiction.

2.4 "**Personal Data**" means any information relating to an identified or identifiable Data Subject that is collected, transferred, or Processed in connection with the Agreement and this DPA, and that is classified as personal data under Data Protection Legislation (as amended or replaced from time to time), or as specified in the Agreement.

2.5 "**Standard Contractual Clauses**" means the standard contractual clauses annex to the EU Commission Decision approved 4 June 2021, for the transfer of Personal Data to processors established in Third Countries (and any successor clauses).

2.6 "**Third Countries**" means countries outside of the European Union/European Economic Area which are not recognized as countries providing adequate protection of Personal Data.

2.7 "**Controller**," "**Data Subject**," "**Personal Data Breach**," "**Processing**," "**Processor**," and "**Supervisory Authority**" shall be interpreted in accordance with the GDPR or other applicable Data Protection Legislation in the relevant jurisdiction.

3. INTERPRETATION

3.1 The provisions of the DPA (in particular, the provisions regarding governing law and jurisdiction) apply to this DPA. If there is any conflict or inconsistency between this DPA and the Agreement, the provisions contained in this DPA shall prevail to the extent of the inconsistency, provided always that nothing in this DPA shall permit Processor to Process Personal Data in a manner prohibited by the Agreement, nor shall this DPA narrow or reduce the scope of any Processor obligations under the Agreement (including the definitions in the Agreement applicable to Personal Data or Personal Data Breach). The Parties hereby agree that the Agreement is amended accordingly to give effect to this Section 3.1.

3.2 To the extent that a term of this DPA requires the performance by a Party of an obligation "in accordance with Data Protection Legislation" (or similar), this term requires performance in accordance with such Data Protection Legislation as is in force and applicable at the time of performance and, if the relevant obligation is not then a requirement under applicable Data Protection Legislation, it shall not apply until it is so required.

4. PROCESSING

4.1 **Processing Personal Data.** The Parties agree that the subject matter and details of Processing of Personal Data are set forth in the Agreement (attached) and/or this DPA, (including Annex 1). Processor shall Process Personal Data for the duration of the Agreement (unless otherwise agreed in writing) only (a) as necessary to effect Processor's obligations under the Agreement; and/or (b) on documented and customary instructions from Controller, unless otherwise required by Applicable Law(s). Processor shall notify Controller if Processor believes such instruction(s) violate(s) applicable Data Protection Legislation.

4.2 **Processor Personnel.** Processor shall take reasonable steps to ensure that access to Personal Data is limited on a need to know/access basis, and that all Processor personnel (including sub-processors) with such access are competent to handle the Personal Data and subject to confidentiality obligations with respect to Controller's Personal Data.

4.3 **Sub-Processing.** With respect to any sub-processor:

4.3.1 Processor shall ensure that the sub-processor is committed, by written contract, to provide the level of protection for Personal Data required by the Agreement, this DPA, and Applicable Law(s); and

4.3.2 Controller agrees that Processor may engage either Xcitium Affiliated companies or third party providers as sub-Processors under this Addendum and hereby provides Processor with a general written authorization for the engagement of such sub-processors in the provision of services. Processor will restrict the processing activities performed by sub-Processors to only what is strictly necessary to provide the services to Controller. Processor shall impose appropriate contractual obligations in writing upon the sub-Processors that are no less protective than this Addendum. Processor makes available to Controller a list of all sub-Processors used by Processor in the provision of service, which is available upon written request and subject to confidentiality and security obligations.

4.3.3 In the event additional sub-Processors are engaged by Processor after the Effective Date of the Agreement, Processor shall notify Controller (in a manner consistent with the confidentiality and security obligations between the Parties) and Controller has a right to object to the newly added sub-Processor by providing written notice to Processor of the objection and reasons therefore within ten (10) business days and require Processor not to use the particular sub-Processor for data processing activities with respect to Controller under the Agreement.

5. DATA SUBJECT RIGHTS

5.1 Processor shall (a) assist Controller to fulfill Controller's obligations regarding a Data Subject's request to exercise his or her rights, as applicable, under applicable Data Protection Legislation (*e.g.*, rights of access, rectification, erasure, restriction of processing, data portability, objection, etc.); and (b) immediately notify Controller if it receives a request from a Data Subject to exercise his or her rights, as applicable, under applicable Data Protection Legislation regarding Personal Data. See also, section 8.1.4, incorporated into this section by reference.

6. INFORMATION SECURITY

6.1 **Information Security.** Processor shall implement reasonable and appropriate technical and organizational measures to provide an adequate level of security and protect Personal Data against unauthorized or unlawful Processing or a Personal Data Breach. Without limiting the foregoing, such technical and organizational measures may be set forth in the Agreement and/or this DPA (including Annex 2).

6.2 **Personal Data Breach.** In the event Processor becomes aware of a Personal Data Breach involving Personal Data, it shall:

6.2.1 Immediately notify Controller of (a) the nature of the Personal Data Breach and any actions taken (or proposed to be taken) to address or mitigate the Personal Data Breach; (b) the number of individuals, the location of the individuals potentially affected (if known) and types of Personal Data concerned; (c) contact information for Processor's data protection officer or other relevant contact who can provide additional information; and

6.2.2 Assist Controller in meeting its obligations under applicable Data Security Legislation.

7. TRANSFERS OUTSIDE THE EUROPEAN UNION/EUROPEAN ECONOMIC AREA

7.1 Processor shall only transfer Personal Data from the European Union to a country outside the European Economic Area (a) with Controller's prior written approval to such transfer; and (b) pursuant to an approved data transfer mechanism. The Parties shall use an appropriate data transfer mechanism, which may include (c) a determination of "adequacy" for the country in which Processor processes the Personal Data, and in the event a country is determined not adequate for this clause (c), additional safeguards for transfer mechanisms shall be included with the technical and organizational measures (Annex 2); (d) Standard Contractual Clauses, set out in Annex 3 to this DPA; or (e) other data transfer mechanisms approved under applicable Data Protection Legislation. For this DPA, the Parties will rely on either clause (c), clause (d), or clause (e) above.

7.2 The agreed-upon data transfer mechanism shall apply for any Personal Data that originated in the European Union or relates to Data Subjects based in the European Union. No transfer of Personal Data from inside the European Union to a country outside the European Economic Area shall take place prior to the implementation of the agreed-upon data transfer mechanism.

7.3 In case of any conflict or inconsistency between the provisions of this DPA and the agreed-upon data transfer mechanism, or in the event that the data transfer mechanism imposes more onerous obligations than the provisions of this DPA, the provisions contained in the data transfer mechanism shall prevail to the extent of the inconsistency, provided always that nothing in the data transfer mechanism shall permit Processor to Process Personal Data in a manner prohibited by this DPA or the Agreement.

8. DATA PROTECTION IMPACT ASSESSMENT AND OTHER OBLIGATIONS

8.1 In relation to Processing of Personal Data by Processor, Processor shall, at the written request of Controller:

8.1.1 Assist Controller with any data protection impact assessments or prior consultations with Supervisory Authorities, as required under applicable Data Protection Legislation;

8.1.2 Make available to Controller all information necessary to demonstrate compliance with Processor's obligations under applicable Data Protection Legislation, this DPA, and the Agreement; and

8.1.3 Contribute to any audits.

8.1.4 Controller has the right, in coordination with Processor, to carry out checks or have auditors or inspectors, in particular cases. Controller has right to ensure compliance with the Agreement by Processor.

9. DELETION OR RETURN OF PERSONAL DATA

9.1 Upon termination or expiration of the Agreement, at Controller's option, Processor shall delete or return all Personal Data, including any existing copies thereof in Processor's possession, unless Applicable Law(s) require(s) otherwise.

10. GENERAL

10.1 Severance. Should any provision of this DPA be held invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (a) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.

10.3 Equitable Relief. Processor acknowledges that any breach of its covenants or obligations set forth in this DPA may cause Controller irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Controller may be entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance, and any other relief that may be available from any court, in addition to any other remedy to which Controller may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive, but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this DPA to the contrary.

10.5 Signature. By signing below, each Party acknowledges that it has carefully read and fully understands this DPA, and each agrees to be bound by the terms of this DPA. This DPA may be signed in counterparts, using an electronic or handwritten signature, which constitute one copy and are of equal effect, whether on original or electronic copies.

IN WITNESS WHEREOF, the undersigned Parties agree to be bound by this DPA as of the Effective Date.

Controller Signature

Controller Name:
Signature:
Name (printed) and Title:
Date Signed:

Processor Signature

Processor Name: Xcitium Inc. 200 Broadacres Drive Second Floor Bloomfield, NJ 07003

Signature:
Name (printed) and Title:
Date Signed:

ANNEX 1:
Subject Matter and Details of Processing

Data Controller / Exporter: The data export is (please specify briefly your activities relevant to the transfer):

The data exporters are the EU affiliates of
_____ as listed in Annex 4

Data Processor / Importer: The data processor/ importer is:

The data importer(s) is Xcitium Inc., part of a global group of companies providing internet security and cybersecurity providing services to Controller that involve Controller's data

Data Subjects: The personal data transferred may concern the following categories of data subjects, as further specified in the Agreement

___X___ Customer's employees, representatives, customers, vendors, and/or any other business contacts including senders and recipients of emails, as applicable.

_____ Other [to be identified by Controller]

Categories of Data: The Personal Data transferred concern (but are not limited to) data described in the product or services Agreement.

- Other data reasonably required to implement the services and performance requested by Controller under the Agreement.

Special Categories of Data: The Personal Data transferred will not include sensitive personal data including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation.

Processing Operations: The Personal Data transferred will be subject to the following basic processing activities:

- Processing activities in the performance of the services as set forth in the Agreement, which is product/service dependent, but may include.
- Endpoint Protection
- Remote monitoring and management.
- Remote access and control
- Service desk and ticketing
- Patch management

ANNEX 2:
Technical and Organizational Security Measures

Processor maintains policies and procedures in support of its privacy and security program including: Information Security Policy, Risk Assessment Policy & Procedures, Business Continuity Plan, Remote Access & Bring Your Own Device (BYOD) Policy, Access Control & Password Policy, Clear Desk & Screen Policy, Third Party/Outsourcing Policy & Procedure, Supplier Due Diligence Policy & Questionnaire, Data Retention & Erasure Policy, Data Protection Policy & Procedure, and Asset Management Policy.

Information and physical security is the protection of the information and data that the Processor creates, handles and processes in terms of its confidentiality, integrity and availability from threats, internally and externally. Information security is an enabling mechanism for information sharing between parties.

Processor is committed to preserving information security of all physical, electronic and intangible information assets across the business, including, but not limited to all operations and activities. We aim to provide information and physical security to: protect customer, 3rd party and client data; preserve the integrity of the Processor and our reputation; comply with legal, statutory, regulatory and contractual compliance; ensure business continuity and minimum disruption; minimize and mitigate against business risk.

Additional and supplemental technical and organizational security measures are used as necessary based on the product/service and may include requiring data encryption of any personal data by state of the art encryption before submission to Processor; data pseudonymization; decryption of data only in an adequate destination country and jurisdiction when in transit; split and multi-party processing with separate batches of data sent to separate entities in separate jurisdictions; Organizational measures can include internal policies for implementation of the technical measures; organization methods; data minimization methods; transparency and accountability measures, and adoption of standards and best practices.

ADDITIONAL TECHNICAL AND ORGANIZATIONAL MEASURES

1. Summary

1.1 These technical and organizational measures may be amended from time to time to follow industry or regulatory changes including any new legislative or regulatory requirements, or industry standards e.g. ISO 27001, PCI DSS, SOC1 (SSAE18), or other standards ("Regulatory Requirements") implemented by various entities. These measures may also vary for a particular product or service as the case may require.

1.2 Either Party may request a change to these measures to ensure continuous compliance with any Regulatory Requirements ("Mandatory Changes"). Each Party shall bear their own costs for implementing Mandatory Changes and shall provide to the requesting Party an implementation plan or confirmation of compliance within sixty (60) calendar days from the date the request was made.

1.3 If a Party requests changes that are not Mandatory Changes then the Parties shall discuss and agree on costs and implementation plan in good faith within sixty (60) calendar days from the date the request was made.

1.4 If a Party is unable to comply with Mandatory Changes, the other Party may elect to terminate the Main Agreement upon written notice without notice period.

2. Security Requirements

Processor will adhere to the following:

2.1 Processor will make their staff or any authorized third party sub processor working on the Controller engagement aware of the applicable security and privacy policies, acceptable use policies, security standards and procedures as well as consequence of nonconformance with them.

2.2 Processor will retain evidence that its staff and any authorized third party (sub processor) has individually read and acknowledged the applicable security and privacy policies, acceptable use policies, security standards and procedures as well as consequence of nonconformance, prior to have access to Controller systems or systems managed by the Processor on behalf of Controller.

2.3 Processor will be responsible for the security of the service/data in scope (as per the regulations/standards applicable to Controller) on behalf of Controller.

2.4 Processor will promptly notify Controller in case staff working on the Controller engagement are leaving the engagement or changing roles within the engagement.

2.5 Processor will perform, at least once per year, an assessment to confirm their staff's compliance with applicable security policies, standards and procedures and report results to Controller (non-compliance can lead to termination of the agreement with Controller).

2.6 Processor will stipulate any outsourced processes affecting the Controller engagement.

2.7 Processor will report any security incidents/problems affecting the Controller engagement not later than 24 hours after having become aware of it, except for crisis mode (e.g. with a possible reputational impact or triggering potential liability under the law) where Controller has to be informed immediately.

2.8 Processor will have anti-virus scan for email (including email attachments).

2.9 Processor will have portable media containing Controller information encrypted (laptop, USB dongle, portable Hard drive, tablet, smartphone, etc.)

2.10 If personal data is accessed and/or processed, Processor will keep an up-to-date documented record of the personnel authorized to access the personal data, indicating their roles and privileges provided to them (including monitoring function and authorization delegation).

2.11 If personal data is accessed and/or processed, Processor will have a formal authorization from Controller to store personal data in portable devices or process personal data outside the premises where the files are located (authorization will set out specific user or user profile, and the duration of its validity).

2.12 If personal data is accessed and/or processed, Processor will implement rules and procedures to ensure that personal data processed on behalf of Controller is processed in accordance with Controller' processing instructions.

2.13 If a system is managed by the Processor for Controller, Processor will ensure the system is compliant with applicable security policies and standards.

2.14 If a system is managed by the Processor for Controller and the user management is done by the Processor, the system will be integrated in the leaver/change of job process of Controller (Processor will ensure user access to the system is revoked when no longer required).

2.15 If a system is hosted by the Processor for Controller, the system will be located in secure areas where physical access attempts are monitored.

2.16 If a system is managed by the Processor for Controller, the system will be hardened, promptly security patched (i.e. security patch documented, tested, and with a fall-back plan prior to production), known vulnerabilities promptly addressed and obsolescence managed.

2.17 If a system is managed by the Processor for Controller, the system will have availability as part of the architecture and disaster recovery plan designed to ensure its ability to fulfil its obligations and that it can be re-instated in case of an event affecting business operations.

2.18 If backups for a system are done by the Processor for Controller, backups will be secured according to the classification of the information they hold, and stored in a separate location from the system. Restoration tests will be performed at least once a year and the results will be provided to Controller.

2.19 If a system is managed by the Processor for Controller and this system is shared between customers, segregation between customers through security controls will be in place.

2.20 If a system is managed by the Processor for Controller, the Processor should have a test environment different than production and tests will be performed in this test environment without any sensitive data. In the exceptional case of usage of a real data (even a copy), the same level of Security as on the production environment will apply.

2.21 If a system is managed by the Processor for Controller, the Processor will undergo an internal or external audit/security assessment and a penetration test at least every year and any necessary corrective measures must be implemented by Processor.

2.22 If a system is managed by the Processor for Controller and this system is managing user password locally (i.e. within the system), security measures will be put in place to ensure adequate password management (renewal of password after first login of the users, usage of complex passwords, password length, etc.)

2.23 If a system is managed by the Processor for Controller, access to data, systems, equipment and documents will be provided based on the "need to know" and "need to handle" principle.

2.24 If a system is managed by the Processor for Controller, multi-layer defence will be in place at different levels (network level, operating systems level, application, etc.)

2.25 All temporary and permanent copies of documents and/or data will comply with the same security measures as the original ones and should be erased or destroyed once they are no longer necessary for the purposes for which they were created.

2.26 If a system is managed by the Processor for Controller, an intrusion detection system will be in place to monitor and report network/system activities for malicious activities or policy violations. This intrusion detection system will be updated every 6 months at minimum.

2.27 If a cloud based system managed by the Processor for Controller, the Processor will provide the applicable security policies upon written request regarding the services offered to Controller (e.g. system & application security, security of information and acceptable use policy, data privacy and data management), and if necessary aligned with Controller policies and standards.

2.28 If a cloud based system is managed by the Processor for Controller, the Processor will provide compliance report at least once per year to Controller on the applicable security policies regarding the services offered to Controller.

2.29 If a cloud based system is managed by the Processor for Controller, the Processor will be ISO 27001 certified during the period of engagement.

2.30 If a cloud based system is managed by the Processor for Controller and the service is relevant for PCI DSS, the Processor will be PCI DSS certified during the period of engagement.

2.31 If a cloud based system is managed by the Processor for Controller and the service has an impact on financial service, the Processor will be covered by SOC1 Type II report during the period of engagement.

2.32 If a system is managed by the Processor for Controller, personal data will be encrypted at rest and in transit.

2.33 If personal data is accessed and/or processed and if a system is managed by the Processor for Controller, usage monitoring will be in place (i.e. actions performed by users, or processes performed by the system for users, are logged sufficiently to provide accountability).

2.34 If personal data is accessed and/or processed and if a system is managed by the Processor for Controller, move of media containing personal data will be explicitly authorized in writing by Controller.

2.35 If personal data is accessed and/or processed and if a public/hybrid cloud based system is managed by the Processor for Controller, the Processor will adhere and comply to the international code of practice for cloud privacy (ISO 27018) which governs the processing of personal information by cloud service providers.

2.36 If non-Controller workstations are used to access or store Controller information, these workstations will have their hard drive encrypted.

2.37 If non-Controller workstations are used to access or store Controller information, these workstations will be under processes to ensure that they are not affected by public security vulnerabilities and protected from intrusion (anti-malware, anti-virus, security patch, etc.)

2.38 If non-Controller workstations are used to access or store Controller information, these workstations will be locked automatically after maximum 15 minutes idleness.

2.39 Processor will ensure that the network they use to access to data managed or owned by Controller from outside of Controller is encrypted, whether public or private.

2.40 If the network is managed by the Processor, wireless network will be encrypted and access to it protected at the same level as the Controller standard.

2.41 If the network is managed by the Processor, security events will be logged according to written policy.

2.42 If a network is managed by the Processor and connected to Controller, access to this network will be secured from people not working on the Controller engagement (e.g. segmentation, access control list, firewall with a rule set following the "least privilege" principle, etc.)

2.43 If a network is managed by the Processor and supporting critical services provided to Controller (e.g. security services or WAN network), Service Level Agreement will be established in the contract with Controller.

2.44 The Processor will notify Controller prior to any material change to the provision of services by the Processor (whether due to business, legal, regulatory, architectural, or other reasons).

2.45 Processor will perform background checks for personnel involved in Controller engagement, before granting access to any Controller facilities/systems, and if requested in writing, deliver to Controller a report describing the background checks that were performed and the results of the same. These should include at least the following, where allowed by applicable laws and regulations:

a) Review of criminal background in all local jurisdictions in which Processor's employee resided for the preceding seven (7) years

b) Verification (for completeness and accuracy) of the curriculum vitae

c) Verification of prior employment for the preceding five (5) years

d) Verification of highest educational level reported

e) Independent identity verification (passport or national ID document)

2.46 Controller reserves the right to audit the Processor no more than once per year upon reasonable written notice including the obligation of Processor to, at Controller' request, provide documentary evidence of compliance with the applicable SR and/or other contractual requirements. The audit may be conducted by a third party selected by Controller. The action plans and costs resulting from it will be borne by the Controller.

2.47 All software provided by the Processor, including third party embedded software, will be protected from all known vulnerabilities by having the latest security patches installed and following industry best configuration hardening standard (SANS, NIST, etc.) For software provided by Processor, all security patches will be made available to Controller immediately upon release. For third party embedded software, critical security patches will be made available to Controller within 7 days and non-critical security patches within 30 days of release.

2.48 If a system is managed by the Processor on behalf of Controller, Controller reserves the right to perform a security assessment/penetration test on the managed system upon reasonable written notice and no more than once per year, which could be conducted by a third party selected by Controller. The action plans and costs resulting from it will be borne by the Controller.

ANNEX 3:
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:

Affiliates listed in Annex 4

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Name of the data importing organisation: Xcitium Inc.

Address: 200 Broadacres Drive, Second Floor, Bloomfield, NJ 07003

Tel.:+1 (973) 859-4000

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.

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least ten days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[4] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) 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 personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the

essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date: _____

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Xcitium Inc.

   200 Broadacres Drive, Second Floor

   Bloomfield, NJ 07003

Contact: Fatih Orhan, Chief Operating Officer

Activities relevant to the data transferred under these Clauses:

In accordance with the Agreement bewteeen the Parties contracted for products and services and legitimate business purposes and interests thereof.

Signature and date: _____

Role (controller/processor): Processor

2. ITarian, LLC

200 Broadacres Drive, Second Floor

Bloomfield, NJ 07003

Contact: Fatih Orhan

Signature and date: _____

Activities are in accordance with the Agrement bewteeen the Parties contracted for products and services, and the legitimate business purposes and interests thereof.

3. NuRD LLC

200 Broadacres Drive, Second Floor

Bloomfield, NJ 07003

Contact: Fatih Orhan, Manager

Signature and date: _____

Activities are in accordance with the Agrement bewteeen the Parties contracted for products and services, and the legitimate business purposes and interests thereof.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

_____ Customer's employees, representatives, customers, vendors, and/or any other business contacts including senders and recipients of emails, as applicable.

_____ Other [to be identified by Controller]

Categories of personal data transferred

The Data transferred concern (but are not limited to) data described in the product or services Agreement.

- Other data reasonably required to implement the services and performance requested by Controller under the Agreement.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable.

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

Continuous on going basis.

Nature of the processing

Customer support and product features in accordance with the Agreement signed by the Parties.

Purpose(s) of the data transfer and further processing

In furtherance of and in order to satisfy the legitimate business and services as stated in the Agreement between the Parties.

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

The data will be retained in accordance with the Agreement and according to applicable law.

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

Processing activities in the performance of the services set forth in the Agreement and for the duration thereof.

C. COMPETENT SUPERVISORY AUTHORITY

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

European Union, with Ireland as the location, and for law and jurisdiction of disputes.

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

The technical and organisational measures implemented by the data importer(s) 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 include the following:

Measures for: ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services; ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; the protection of data during transmission; the protection of data during storage; ensuring events logging; ensuring system configuration, including default configuration; internal IT and IT security governance and management; assurance of processes and products

Processor maintains policies and procedures in support of its privacy and security program including: Information Security Policy, Risk Assessment Policy & Procedures, Business Continuity Plan, Remote Access & Bring Your Own Device (BYOD) Policy, Access Control & Password Policy, Clear Desk & Screen Policy, Third Party/Outsourcing Policy & Procedure, Supplier Due Diligence Policy & Questionnaire, Data Retention & Erasure Policy, Data Protection Policy & Procedure, and Asset Management Policy.

Information and physical security are the protection of the information and data that the Processor creates, handles and processes in terms of its confidentiality, integrity and availability from threats, internally and externally. Information security is an enabling mechanism for information sharing between parties.

Processor is committed to preserving information security of all physical, electronic and intangible information assets across the business, including, but not limited to all operations and activities. We aim to provide information and physical security to: protect customer, 3rd party and client data; preserve the integrity of the Processor and our reputation; comply with legal, statutory, regulatory and contractual compliance; ensure business continuity and minimum disruption; minimize and mitigate against business risk.

For transfers to (sub-) processors, the specific technical and organisational 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:

Same as above.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

a. Amazon Web Services
Frankfort, Germany

b. Comodo Security Solutions Ltd.
176-178 Pontefract Road, Cudworth, Barnsley, South Yorkshire, England, S72 8BE

c. Xcitium Inc.
200 Broadacres Drive, Second Floor

Bloomfield, NJ USA 07003

Contact: Fatih Orhan
Chief Operating Officer
fatih@xcitium.com

d. ITarian, LLC
200 Broadacres Drive, Second Floor

Bloomfield, NJ USA 07003

Contact: Fatih Orhan
fatih@xcitium.com

e. NuRD LLC
200 Broadacres Drive, Second Floor

Bloomfield, NJ USA 07003

Contact: Fatih Orhan, Manager
fatih@nurd.com

ANNEX 4:
Controller Affiliates

NAME	ADDRESS

Agreement Appendix

(Agreement between the Controller and Processor to be attached here.)