ttec.com

TTEC'S SECURITY REQUIREMENTS

CONTRACTOR SECURITY REQUIREMENTS

1. Definitions

Capitalized terms appearing in the Master Services Agreement shall have the same meaning as they have in the Master Services Agreement. Capitalized terms not appearing in the Master Services Agreement shall have the following meanings:

- **Contractor Personnel** means any employee, independent contractor, consultant, or subcontractor of or acting on behalf of Contractor.
- **Process or Processes or Processing** means the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- **Personal Data** means any data that identifies or can be used to identify an individual.
- Payment Card Information (PCI) means any information that is associated with a person's payment credit or debit card. Payment card information includes (but not limited to) primary account number (PAN), cardholder name, expiration date, or Card Verification Code (CVC).
- **TTEC Data** means any data provided to Contractor or created by Contractor by or on behalf of TTEC. TTEC Data includes Client Data, if any.
- **Client Data** means any data provided to TTEC by any of TTEC's clients.
- **Protected Health Information** means individually identifiable information that relates to a person's past, present, or future physical or mental health and was created or received by a health care Contractor, health plan, employer, or health care clearinghouse.
- **HITRUST** means the Health Industry Trust Alliance (HITRUST) Common Security Framework (CSF), as required.

2. Information Security Program

Contractor, and all applicable Contractor Personnel, shall implement and maintain a comprehensive written information security program, including an information security policy. The program will contain appropriate administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of TTEC Data in Contractor's custody or control. The program will also include the appointment of a single person with sufficient authority who is responsible and accountable for the provisions outlined below.

Contractor will regularly test or otherwise monitor the effectiveness of the safeguards, controls, systems, and procedures. Contractor will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of TTEC Data, and ensure that there are safeguards in place to control those risks.

Contractor will develop, implement, and maintain privacy policies and procedures that are designed to enable Contractor to comply with the requirements of this Exhibit ("Information Security Program").

As requested by TTEC, Contractor will supply a copy of its written privacy and information security policies and procedures to TTEC.

Contractor will conduct background investigations of Contractor Personnel, as appropriate. No employee, Contractor Personnel or consultant hired shall be given access to TTEC Data until such investigation is complete and the results are acceptable.

Contractor will conduct privacy and information security training, as appropriate, for Contractor Personnel that at least meet the requirements set out in this Exhibit. The training will be conducted at reasonable intervals to periodically reinforce awareness of privacy and information security issues.

Contractor will supply enhanced privacy and information security training to Contractors who interact directly with TTEC Data. Such training shall be specific to the appropriate protection and handling of data as prescribed by applicable regulatory frameworks, or by law. For employees that have access to Protected Health Information, Contractor will train its employees on the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA).

Contractor will ensure that any of its employees, Contractor Personnel or consultants who handle TTEC Data have signed or will sign a confidentiality agreement with confidentiality and non-disclosure terms no less restrictive than those contained in the Master Services Agreement.

Contractor will monitor all Contractor Personnel for compliance with requirements of this Exhibit.

3. Asset Management, Classification, and Protection

Contractor, and all applicable Contractor Personnel, shall implement and maintain asset management policies, procedures, and tools which (a) identify all equipment and media used in the storage or Processing of TTEC Data; (b) assign responsibility for all equipment and media to one or more custodians; and (c) require regular reviews of the asset inventory for accuracy and to identify missing equipment and media.

Assets must be classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational, and physical safeguards. These may include controls such as access management, encryption, logging and monitoring, and data destruction.

To protect against malicious use of assets and malicious software, additional controls must be implemented based on risk. Such controls should include, but are not limited to, information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; data loss prevention; system compliance scans; intrusion prevention monitoring and response; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; system and application patch management; and system and application vulnerability scanning and management.

4. Security Training and Awareness

Contractor, and all applicable Contractor Personnel, shall implement and maintain Awareness and Training policies, procedures, and tools which address (a) information security threats and best practices; (b) information security policies, procedures, and controls in place to protect TTEC Data; and (c) each Contractor Personnel's roles and responsibilities in the protection of TTEC Data. Contractor Personnel shall be trained on these policies and procedures within thirty (30) days of hire and minimally on an annual basis thereafter while in a role responsible for the protection of TTEC Data.

5. Hardware and Software Installation and Maintenance

Contractor, and all applicable Contractor Personnel, shall implement and maintain system and application maintenance policies, procedures, and tools, including controls related to (a) structured vulnerability management, including regular scanning, penetration testing, risk analysis, and timely patching; (b) change management, including documentation of the purpose, security impact analysis, testing plan and results, and authorization for all changes; (c) configuration management, including secure baseline configurations; and (d) monitoring to detect and generate alerts for unauthorized changes.

6. Access Controls

Contractor shall ensure that access to TTEC systems is restricted, based on procedures to ensure appropriate approvals. To reduce the risk of misuse, intentional or otherwise, access is provided based on role, segregation of duties, and least privileges. Access to corporate systems and data should be on a "need to know" basis only with access revoked immediately upon termination or transfer into a role which no longer requires access to TTEC Data.

Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place using two factor authentication solution.

Specific event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

7. Security Incident Management

Contractor must notify TTEC promptly, but in no event later than twenty-four (24) hours, upon initial detection or a reasonable suspicion of a Security Incident. Security Incident notifications must be sent to TTEC's Security Operations Center (SOC) at securityoperationscenter-infosec@ttec.com and contact TTEC's Security Operations Center at 1-833-883-2762 for further details. Such notification will summarize in reasonable detail the circumstances of the Security Incident including (i) the date and time period of the Security Incident; (ii) the impact of such Security Incident on TTEC and, if applicable, individuals whose Personal Information is affected by such Security Incident, including an estimate of the number of individuals affected and a description of the Personal Information involved; (iii) what (if any) corrective action has been taken by Contractor; (iv) what steps Contractor has taken to isolate the Security Incident; and (v) any additional details that may be necessary for TTEC to isolate the Security Incident or prevent any further adverse effect of the Security Incident. Contractor will also promptly undertake an investigation of such Security Incident and cooperate with TTEC in connection with such investigation, including by (x) providing TTEC with physical access to the facilities and operations affected; (y) facilitating interviews with relevant Contractor Personnel or others who perform work for Contractor; (z) preserving and promptly making available to TTEC upon request all relevant executive records, logs, files, data reporting, and other materials and documentation relevant to TTEC's investigation; (aa) promptly complying with any reasonable requests that TTEC may make (e.g., changing security credentials) and (bb) providing regular updates to TTEC as material additional information becomes available and providing TTEC with additional information that it may request, in each case, relating to the Security Incident.

Upon receipt of notice of a Security Incident, TTEC may take all reasonable and appropriate steps to (i) protect TTEC Confidential Information; (ii) execute its obligations under Applicable Data Protection Laws; and (iii) implement its Computer Incident Response Plan, including Contractor performing an audit of Contractor's Security Measures or the security safeguards of any Approved Subcontractors or both. Contractor will not impede and will cooperate with and undertake all commercially reasonable efforts to assist with, TTEC's activities pursuant to the forging sentence. Contractor will promptly reimburse TTEC for all costs and expenses (including attorneys' and other legal fees) reasonably incurred by TTEC in connection with a Security Incident caused by any breach of Contractor's obligations under this Agreement or any other acts or omissions of Contractor, including in connection with remediation efforts.

TTEC has the sole right to determine: (i) whether notice of a Security Incident is to be provided to any non-party (e.g., individuals, TTEC Regulators, law enforcement agencies, consumer reporting agencies); (ii) the contents of any such notice; and (iii) whether any type of remediation may be offered to affected individuals, and the nature and extent of any such remediation. Except with TTEC's prior written consent, or required by Applicable Data Protection Laws, Contractor may not disclose the Security Incident to, or otherwise notify, any third party (other than its insurers, attorneys and other confidential advisors who are assisting Contractor in connection with such Security Incident).

8. Data Encryption

Contractor agrees that all TTEC Data will be encrypted using an industry standard encryption solution while the data is in transit or at rest. Further, Contractor agrees to backup all TTEC Data as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Contractor further agrees that any and all TTEC Data that could be considered Protected Health Information or personally identifiable information under current legislation or regulations stored on any portable or laptop computing device or any portable storage medium be likewise encrypted. Encryption solutions will be deployed with no less than AES 256-bit key for symmetric encryption and a 2048-bit (or larger) bit key length for asymmetric encryption.

9. Data Security Obligations

Contractor warrants and undertakes that Contractor Personnel have in place and shall maintain appropriate industry standard physical, organizational, and technical processes and procedures to protect against any Data Breach, in particular where the Processing involves the transmission of data over a network or storage of data at rest, and against all other unlawful forms of Processing of TTEC Data (collectively, "Appropriate Safeguards"). In addition, at any point during the term of the Master Services Agreement, Contractor shall, upon request, provide TTEC with a copy of Contractor Personnel's applicable security standards, policies, procedures, and guidelines. These policies may include, but are not limited to risk management, asset management, access control and identity management, security awareness and training, contingency planning, system maintenance and patching, and media protection. Contractor Personnel shall regularly, but in no event less than annually, evaluate, test and monitor the effectiveness of their Appropriate Safeguards and shall promptly adjust and/or update their Appropriate Safeguards as reasonably warranted by the results of such evaluation, testing, and monitoring.

10. Employee Background Checks

Contractor agrees to perform background checks prior to allowing access on those employees who will have access to TTEC Data or to systems which maintain or transmit TTEC Data. Such background checks will include verification of the employee's authorization to work, and a seven (7) year state and local criminal check of those states and counties where the employee resided. For employees located outside of the United States, Contractor shall perform a functionally equivalent background check to the extent permitted by local law.

11. Client Security Requirements

In the event that Contractor processes Client Data, Contractor agrees to adhere to any additional security provisions required by the applicable TTEC client(s). Client security provisions will not apply to Contractor prior to TTEC providing such security provisions to Contractor.

12. Certifications and Audits

No more than annually and with thirty (30) days written notice, TTEC may audit Contractor's compliance with this Exhibit, any client security requirements, TTEC may audit Contractor's compliance with this Exhibit, any security client, and any other regulatory requirements applicable to Contractor's Processing of TTEC Data. Such audits may consist of questionnaires, interviews and/or site visits.

If Contractor processes Protected Health Information (PHI) data or data within the scope of the TTEC HITRUST certification environment, Contractor is also subject to the additional requirements in the HITRUST Exhibit, as applicable.

If Contractor Processes payment card data, Contractor agrees to maintain a third-party Payment Card Industry Data Security Standards (PCI-DSS) certification and to provide a copy of the attestation of compliance issued by a recognized PCI Qualified Security Assessor (QSA) to TTEC upon request. Further, if Contractor Processes Personal Data, Contractor agrees to provide TTEC with a copy of its most recent ISO 27018:2014, ISO 27001:2013, SOC 2 Type II report or equivalent recognized independent compliance attestation annually. If Contractor does not have the required certification(s), Contractor agrees to obtain such certification(s) within six (6) months of the date of the Agreement. Contractor must maintain such certification(s) for the term of the agreement.

TTEC may revoke Contractor's access to TTEC information systems and/or TTEC Data if Contractor fails to participate in any audits, fails to maintain any applicable PCI-DSS certification or equivalent recognized industry compliance certification(s) or submit a copy of its industry compliance certification(s) and attestations of compliance to TTEC at least annually or fails to comply with any provisions of this Exhibit.

13. Derivative Data

Contractor will not use TTEC Data or data derived from TTEC Data without the express, written consent of TTEC. If Contractor will have access to data ultimately belonging to a client of TTEC, then Contractor will not use such data or data derived from the client's data without the express, written consent of the applicable client.

EXHIBIT B
TTEC'S SECURITY REQUIREMENTS (Cont.)

GLOBAL DATA PRIVACY

1. Definitions

- **Personal Data** means information that identifies or can be used, directly or indirectly, to identify or authenticate an individual.
- **Process or Processes or Processing** means the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- **Sensitive Data** means a subset of Personal Data which consists of an individual's financial or account information, government issued identifier, health or medical characteristics (including biometric and genetic data), sex life, race or ethnicity, religious, moral, or philosophical beliefs, political opinions, or trade union membership or other information that could cause the individual financial or reputational harm.
- **TTEC Data** means any Personal Data and/or Sensitive Data provided to Contractor by TTEC regardless of whether the data belongs to TTEC or TTEC's clients.

2. General Privacy Requirements

A. Contractor will use the TTEC Data only for the purposes set forth in the Master Services Agreement and will not disclose the TTEC Data to any person or entity outside of Contractor without written permission from TTEC. Contractor will not process the TTEC Data in a way that is incompatible with the Agreement.

B. Contractor agrees not to transfer or maintain TTEC Data outside the Greece without the written consent of TTEC.

C. Contractor will use reasonable precautions to protect the TTEC Data from loss, misuse, unauthorized access, disclosure, alteration, or destruction, and will notify TTEC promptly, and in any case within three (3) days, of any such loss, misuse, unauthorized access, disclosure, alteration or destruction.

D. Contractor will notify TTEC promptly, and in any case within three (3) days, about: (i) any legally binding request for disclosure of the TTEC Data by a government entity, court of law, or pursuant to a subpoena, unless otherwise prohibited, and (ii) any request received directly from a Data Subject without responding to the request, unless Contractor has been otherwise authorized in writing by TTEC to do so.

E. Contractor shall promptly: (a) refer to TTEC any individual who contacts Contractor seeking access or correction to or with any inquiries or complaints about his or her Personal Data or Sensitive Data in connection with or otherwise relating to the Services; (b) notify TTEC regarding any such request, inquiry or complaint; and (c) provide all reasonable co-operation, assistance, information and access to Personal Data and/or Sensitive Data in its possession, custody or control as is necessary for TTEC to promptly (and, in any event, within any timeframe required by applicable law) respond to such request, inquiry or complaint.

F. Contractor will: (i) investigate any complaint regarding compliance with this agreement; (ii) implement mechanisms to comply with this agreement; and (iii) remedy problems arising out of failure to comply with this agreement.

G. Contractor shall provide, in a timely manner, all necessary and reasonable information and co-operation to TTEC and to any regulatory bodies or authorities with jurisdiction or oversight over TTEC Data in connection with any investigations, audits or inquiries made by any such regulator. TTEC may be required to disclose (without advance notice or consent) confidential information of Contractor to such Privacy Regulators in connection with any investigation, audit or inquiry that pertains to or involves the Services.

H. The parties will inform each other about any dispute or claim brought by a Data Subject against either or both of the parties and will cooperate with a view toward settling them amicably in a timely fashion.

I. Each party shall be liable to the other for damages it causes by any breach of this Exhibit.

J. Upon termination or expiration of the Agreement, Contractor will destroy all copies of the TTEC Data in its possession in any form and certify such destruction to TTEC in writing. Contractor agrees to provide a copy of any TTEC Data in its possession to TTEC in a mutually agree upon format upon TTEC's request.

3. Compliance with Global Data Privacy Laws

To the extent that Contractor processes data subject to the subject to global data privacy laws, Contractor agrees to comply with the Australian Data Privacy Principals, the Canadian Personal Information and Electronic Documents Act, Costa Rica's Protection in the Handling of the Personal Information of Individuals, the Mexican Federal Law on the Protection of Personal Data Held by Private Parties, the Philippines Data Privacy Act, the New Zealand Privacy Act and similar global data privacy laws.

4. European Union Privacy Requirements

In the event that Contractor will processes TTEC Data that includes the Personal Data and/or sensitive data of residents of the European Union, Contractor represents that it participates in EU-US Privacy Shield and will continue to participate in Privacy Shield for the length of the Agreement. If Contractor does not participate in Privacy Shield or if Contractor receives TTEC's consent to transfer data to countries other than the those that are members of the European Union or the United States, then the EU Standard Contractual Clauses Attachment shall apply.

THE EUROPEAN UNION (EU) STANDARD CONTRACTUAL CLAUSES ATTACHMENT

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.

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 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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

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.

MODULE TWO: Transfer controller to processor

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 ([4]) (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.
(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

MODULE TWO: Transfer controller to processor

(a) 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 1 month 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.
(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. ([8]) 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 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

MODULE TWO: Transfer controller to processor

(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.

MODULE TWO: Transfer controller to processor

(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:

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(a) 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.

(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

MODULE TWO: Transfer controller to processor

(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 ([12]);

(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 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

MODULE TWO: Transfer controller to processor

(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) [For Modules One, Two and Three: 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

MODULE TWO: Transfer controller to processor

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 the Netherlands.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(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 the Netherlands (*specify Member State*).

(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.