

GDPR & DATA PROTECTION SCHEDULE

Under the Agreement, the Customer engages or may engage the Supplier to Process Personal Data on behalf of the Customer. To the extent of that Processing of Personal Data and for the purposes of the Agreement, the Customer is a 'Controller' and the Supplier is a 'Processor' for the purposes of the GDPR. As such, Article 28 of the GDPR requires that the details in this schedule are included in the contract between the Customer and the Supplier.

The parties must set out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of data subjects – see appendix 1 to this schedule.

The terms used in this schedule have the meanings given to them in clause 13 of this schedule. Capitalized terms used in this schedule that are not defined in clause 13 of this schedule have the meaning given to them in the GDPR or in the Agreement.

Headings used in this schedule are for ease of reference only and are not intended to influence the interpretation of a clause.

- **1. Processing of Personal Data**

- 1.1 The Supplier will:

- a. Instructions from Customer: in providing Services under this Agreement, Process Personal Data only on the Customer's documented instructions (as provided in clause 2 and in appendix 1 to this schedule or otherwise in writing) unless required to do so by Member or Union State law which applies to the Supplier in which case the Supplier will inform the Customer of that legal requirement before Processing unless the Supplier is prohibited from informing the Customer by that law;
- b. Confidentiality: ensure that the Supplier's personnel who are authorised to Process the Personal Data have obligations of confidentiality to the Supplier (including as required in clause 3 below) in respect of the Personal Data or are under an appropriate statutory obligation of confidentiality;
- c. Security: comply with the security obligations in clause 4 below;
- d. Subprocessors: comply with the provisions relating to Subprocessors in clause 5 below;
- e. Data subjects' rights: provide assistance to the Customer with responding to data subjects' rights in accordance with clause 6 below;
- f. Assist Customer: comply with its obligations to assist the Customer in relation to security of Personal Data and data protection impact

assessments and prior consultation in accordance with clause 7 below;

- g. Deleting and returning data: after the provision of Services related to Processing of Personal Data has ended, at the choice of the Customer either delete or return to the Customer all of that Personal Data and delete existing copies unless Member or Union State law requires storage of Personal Data in accordance with clause 8 below; and
- h. Compliance and audits: make available to the Customer all information necessary to demonstrate compliance with Article 28 of the GDPR and allow for and contribute to audits including inspections conducted by the Customer or another auditor mandated from time to time, in accordance with clause 9 below. The Supplier will immediately inform the Customer if, in its opinion, an instruction received from the Customer under this clause 1.1(h), infringes the GDPR or other Member or Union State data protection provisions.

- **2. Instructions from Customer**

- 2.2 The Customer instructs the Supplier (and authorises the Supplier to instruct each Subprocessor) to:
 - a. Process Personal Data; and
 - b. in particular, transfer Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with and in compliance with the Agreement.

- 2.2 The Customer warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in clause 2.1 on behalf of the Customer.

- **3. Confidentiality**

- 3.1 The Supplier will take reasonable steps to ensure the reliability of its employees, agents or contractors who may have access to Personal Data, ensuring in each case that access is limited to those individuals who need to know or need to access the relevant Personal Data, as necessary for the purposes of the Agreement, and to comply with applicable laws in the context of that individual's duties to the Supplier, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

- **4. Security**

- 4.1 Subject to clause 4.2 below, the Supplier will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including amongst other things as appropriate:
 - a. the pseudonymisation and encryption of Personal Data;
 - b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
 - d. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.
- 4.2 In assessing the appropriate level of security for clause 4.1 above, the Supplier will take account in particular of the risks of a Personal Data Breach that are presented by the Processing to be undertaken under the Agreement.
- 4.3 The Supplier will in relation to Personal Data:
 - a. implement and maintain appropriate information security to protect Personal Data against:
 - i. a Personal Data Breach;
 - ii. all other unauthorized or unlawful forms of Processing; and
 - iii. any breach of the Supplier's information security obligations in this schedule. The Supplier will (and will ensure that its Sub-processors) provide full cooperation and assistance to the Customer in ensuring that the individuals' rights under the GDPR or applicable Member State laws are timely and appropriately addressed for the fulfilment of the Customer's obligation to respond without undue delay to requests by such individuals as required by Data Privacy Laws, including the rights of subject access, rectification, erasure, and portability, and the right to restrict or object to certain Processing;
 - b. take reasonable steps to inform its staff, and any other person acting under its supervision, of the responsibilities of any Data Privacy Laws due to the incidental access to Personal Data, and ensure the reliability of its staff and any other person acting

under its supervision who may come into contact with, or otherwise have access to and Process, such Personal Data.

- **5. Subprocessors**

- 5.1 The Customer authorises the Supplier to appoint Subprocessors (and permits each Subprocessor appointed in accordance with this clause 5 to appoint Subprocessors) in accordance with this clause 5 and any restrictions in the Agreement.
- 5.2 The Supplier will give the Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within two weeks of receipt of that notice, the Customer notifies the Supplier in writing of any objections (on reasonable grounds) to the proposed appointment, the Supplier will not appoint (nor disclose any Personal Data to) the proposed Subprocessor unless and until it obtains the prior written consent of the Customer.
- 5.3 With respect to each Subprocessor, the Supplier will:
 - a. enter into an agreement with the Subprocessor which includes the same data protection obligations as set out in this schedule (and Appendix 1) and in particular includes sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. If the Subprocessor fails to fulfil its data protection obligations, the Supplier will remain fully liable to the Customer for the performance of that Subprocessor's obligations;
 - b. if the Processing by the Subprocessor will involve a Restricted Transfer, ensure that the Standard Contractual Clauses (in Appendix 2 to this schedule) are at all relevant times incorporated into the agreement between the Supplier and the Subprocessor; and
 - c. provide to the Customer for review, copies of the Supplier's agreements with Subprocessors (confidential commercial information that is not relevant to the requirements of this schedule may be blacked out) as the Customer may request from time to time.
- 5.4 Appendix 1 to this schedule sets out certain information regarding the Supplier's Processing of Personal Data, as required by article 28(3) of the GDPR. The Customer may make reasonable amendments to

Appendix 1 by written notice to the Supplier from time to time as the Customer reasonably considers necessary to meet those requirements.

- **6. Data Subjects' Rights**

- 6.1 Taking into account the nature of the Processing, the Supplier will, by implementing appropriate technical and organisational measures to the extent described in clause 4, assist the Customer to respond to requests to exercise Data Subject rights under the Data Protection Laws.
- 6.2 The Supplier will:
 - a. promptly notify the Customer if the Supplier or any Subprocessor receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and
 - b. ensure that the Supplier or relevant Subprocessor does not respond to that request except on the documented instructions of the Customer or as required by Applicable Laws to which they are subject, in which case the Supplier will to the extent permitted by Applicable Laws inform the Customer of that legal requirement before the Supplier or relevant Subprocessor responds to the request.

- **7. Assist Customer**

- 7.1 Assist Customer with Security of Processing:
 - a. The Supplier will assist the Customer in respect of the Customer's obligations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, by complying with the Supplier's obligations under clause 4 of this schedule.
- 7.2 Assist Customer with notifications of Personal Data Breach
 - a. The Supplier will notify the Customer without undue delay if the Supplier or any Subprocessor becomes aware of a Personal Data Breach, providing the Customer with sufficient information to allow the Customer to meet any obligations to report the Personal Data Breach to the relevant Supervisory Authority under the Data Protection Laws (noting that the Customer is required, where feasible, to notify applicable Personal Data breaches to the relevant Supervisory Authority within 72 hours after having become aware of the breach).

- b. The Supplier will co-operate with the Customer and take such reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.
- 7.3 Assist Customer with communication of Personal Data breach to Data Subject
 - a. Where a Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons:
 - i. such that the Customer is required to communicate the Personal Data Breach to the Data Subject (including where, despite the conditions referenced in clause 7.3(a)(ii) below being met, the Supervisory Authority has required the Customer to communicate the Personal Data Breach to the Data Subject), the Supplier will assist the Customer in doing so by providing all relevant information as may be reasonably required by the Customer;
 - ii. but despite that high risk, the Customer is not required to communicate the Personal Data Breach to the Data Subject due to certain conditions being met (such as that the Personal Data is encrypted and so unintelligible to any person not authorised to access it), the Supplier will assist the Customer by providing all relevant information as may be reasonably required by the Customer.
- 7.4 Assist Customer with Data Protection Impact Assessments
 - a. The Supplier will provide reasonable assistance to the Customer with any data protection impact assessments which the Customer reasonably considers to be required of the Customer by Article 35 of the GDPR or equivalent provisions of related Data Protection Laws. The Supplier's obligations under this clause 7.4(a) are solely in relation to Processing of Personal Data by the Supplier and taking into account the nature of the Processing and information available to the Supplier.
- 7.5 Assist Customer with Prior Consultation with Supervisory Authority
 - a. The Supplier will provide reasonable assistance to the Customer with prior consultations with

Supervising Authorities or other competent data privacy authorities, which the Customer reasonably considers to be required of the Customer by Article 36 of the GDPR or equivalent provisions of related Data Protection Laws. The Supplier's obligations under this clause 7.5(a) are solely in relation to Processing of Personal Data by the Supplier and taking into account the nature of the Processing and information available to the Supplier.

- **8. Deletion or return of Personal Data**

- 8.1 Subject to clauses 8.2 and 8.3, the Supplier will, within four weeks of the date of expiration or termination of Services involving the Processing of Personal Data (the "End of Processing Date"), delete and procure the deletion of all copies of the Personal Data.
- 8.2 Subject to clause 8.3, the Customer may in its absolute discretion by written notice to the Supplier within four weeks of the End of Processing Date require the Supplier to:
 - a. return a complete copy of all Personal Data to the Customer by secure file transfer in such format as is reasonably notified by the Customer to the Supplier; and
 - b. delete and procure the deletion of all other copies of Personal Data Processed by the Supplier. The Supplier will comply with any such written request within four weeks of the End of Processing Date.
- 8.3 The Supplier may retain Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Supplier will:
 - a. ensure the confidentiality of all such Personal Data;
 - b. ensure that such Personal Data is only processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.
- 8.4 The Supplier will provide written certification to the Customer that it has fully complied with this clause 8 within four weeks following the End of Processing Date.

- **9. Audit rights**

- 9.1 Subject to clauses 9.2 to 9.4, the Supplier will make available to the Customer on request all information necessary to demonstrate compliance with this schedule,

and will allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of Personal Data by the Supplier.

- 9.2 Information and audit rights of the Customer only arise under clause 9.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws (including, where applicable, article 28(3)(h) of the GDPR).
- 9.3 The Supplier may, on reasonable grounds, object to the proposed auditor in which case the Customer will propose an alternate auditor.
 - a. The Customer will give the Supplier reasonable notice of any audit or inspection to be conducted under clause 9.1 and will make (and ensure that its auditor makes) reasonable endeavours to avoid causing any damage, injury or disruption to the Supplier's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. The Supplier need not give access to its premises for the purposes of such an audit or inspection for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections which:
 - i. the Customer reasonably considers necessary because of genuine concerns as to the Supplier's compliance with this schedule; or
 - ii. the Customer is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where the Customer has identified its concerns or the relevant requirement or request in its notice to the Supplier of the audit or inspection.

• 10. Restricted Transfers

- 10.1 Subject to clause 10.3, where the Services involve a 'Restricted Transfer', the Customer (as "data exporter") and the Supplier (as "data importer") each agrees to the Standard Contractual Clauses in respect of that Restricted Transfer (see definition but a 'Restricted Transfer' in essence means transferring Personal Data out of the European Union).

- 10.2 The Standard Contractual Clauses will come into effect under clause 10.1 on the later of:
 - a. the data exporter becoming a party to them;
 - b. the data importer becoming a party to them; and
 - c. commencement of the relevant Restricted Transfer.
- 10.3 There is no requirement for the Supplier and Customer to agree to the Standard Contractual Clauses (or to include the Standard Contractual Clauses in the Agreement) where the transfer of Personal Data is to an Approved Jurisdiction.

- **11. Order of precedence**

- 11.1 Nothing in this schedule reduces the Supplier's obligations under the Agreement in relation to the protection of Personal Data or permits the Supplier to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this schedule and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.
- 11.2 Subject to clause 11.1, in the event of inconsistencies between the provisions of this schedule and the Agreement, the provisions of this schedule will prevail.

- **12. Changes in Data Protection Laws**

- 12.1 The Customer may by at least 30 calendar days' written notice to the Supplier:
 - a. vary the Standard Contractual Clauses, as they apply to Restricted Transfers which are subject to a particular Data Protection Law, as required as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and
 - b. propose any other variations to this schedule which the Customer reasonably considers to be necessary to address the requirements of any Data Protection Law.
- 12.2 If the Customer gives notice under clause 12.1(a):
 - a. the Supplier will promptly co-operate (and require affected Subprocessors to promptly co-operate) to ensure that equivalent variations are made to the agreements made under clause 5.3; and
 - b. the Customer will not unreasonably withhold or delay agreement to any consequential variations to this schedule proposed by the Supplier to protect the Supplier against additional risks associated with the variations made under this clause 12.2.

- 12.3 If the Customer gives notice under clause 12.1(b), the parties will promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in the Customer's notice as soon as is reasonably practicable.

- **13. Definitions**

In this schedule:

"Approved Jurisdiction" means a country (or territory or specified sector within it) or an international organisation which the Commission has decided, under Article 45(3) of the GDPR, ensures an adequate level of data protection;

"Contracted Processor" means the Supplier or a Subprocessor

"Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

"Data Subject" means an identified or identifiable natural person, or any updated definition of this term from time to time in the GDPR;

"EEA" means the European Economic Area;

"EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

"GDPR" means EU General Data Protection Regulation 2016/679;

"Information Security Obligations" means commercially reasonable and appropriate physical, technical and organisational security measures (determined with regard to risks associated with the Processing of Personal Data as part of the Services), including the measures set out in the Agreement and in particular in Appendix 2 to this schedule (where applicable).

"Personal Data" means any information related to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person, or any updated definition of 'Personal Data' from time to time in the GDPR;

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, or any updated definition of 'Personal Data Breach' from time to time in the GDPR;

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and 'Process' has a corresponding meaning;

"Restricted Transfer" means transferring Personal Data outside of the European Union, being:

- . a transfer of Personal Data from the Customer to the Supplier or to a Subprocessor; or
- a. an onward transfer of Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer means would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws), in the absence of the Standard Contractual Clauses;

"Services" means the services and other activities to be supplied to or carried out by or on behalf of the Supplier for the Customer under the Agreement;

"Subprocessor" means any person (including any third party, but excluding an employee of the Supplier or any of its sub-contractors) appointed by or on behalf of the Supplier to Process Personal Data on behalf of the Customer in connection with the Agreement;

"Standard Contractual Clauses" means the clauses in Appendix 2 to this schedule;

The terms "Member State", "Union State", "Supervisory Authority" have the meaning given to those terms in the GDPR, and corresponding terms have corresponding meanings.

The word "includes" means 'includes without limitation', and "including" has a corresponding meaning.

APPENDIX 1 TO GDPR SCHEDULE

Details of Processing of Personal Data

This Appendix 1 includes certain details of the Processing of Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Personal Data:

Such data may include your name, your physical address, your billing address, and your email address and for the period whilst we provide the services to you.

The nature and purpose of the Processing of Personal Data:

Such data is captured to provide the services to you, and for billing and support activities.

The types of Personal Data to be Processed:

Such data may include your name, your physical address, your billing address, and your email address.

The categories of Data Subject to whom Personal Data relates:

Such data may relate to current personnel, contractors, website end-users, suppliers, consumers, customers, prospects and application end-users.

The obligations and rights of the Customer:

The obligations and rights of the Customer are set out in this Agreement and this schedule.

APPENDIX 2 TO GDPR SCHEDULE

Standard Contractual Clauses (Processors)

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 and contact details of the data exporting organisation:

Refer definition of 'Customer' in clause 20 of the End User Terms. (the data exporter)
And

Name and contact details of the data importing organisation:

Refer name of Supplier at start of these SaaS End User Terms.
Refer clause 18.1 of the End User Terms for contact details of Supplier. (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.

Background

The data exporter has entered into an Agreement with the data importer. Pursuant to the terms of the Agreement, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is

located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

- a. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- b. 'the data exporter' means the controller who transfers the personal data;
- c. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d. 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e. 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- f. 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

- c. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e. that it will ensure compliance with the security measures;
- f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; [If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.]
- g. to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- h. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- j. that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b. that it has no reason to believe that the legislation applicable to it

- prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
 - d. that it will promptly notify the data exporter about:
 - i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - ii. any accidental or unauthorised access, and
 - iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
 - e. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
 - f. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
 - g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
 - h. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
 - i. that the processing services by the subprocessor will be carried out in accordance with Clause 11;
 - j. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered

damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

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

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - i. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - ii. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in

paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

ANNEX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Annex forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is:

Data importer

The data importer is:

Data subjects

The personal data transferred concern the following categories of data subjects: Personal details relating to the identity and

location of the Customer

Categories of data

The personal data transferred concern the following categories of data: Name, physical address, billing address, email address

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: Not Applicable

Processing operations

The personal data transferred will be subject to the following basic processing activities: In order to provide billing and support activities.

ANNEX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Annex forms part of the Clauses and must be completed and signed by the parties.

For more detailed information on the security measures used by Microsoft in the provision of O365 and Azure services, and in accordance with Clauses 4(d) and 5(c)), please refer to the following links:

[Microsoft Office365 Security](#)
[Microsoft Azure Security](#)