Data Processing Addendum

This Data Processing Addendum (**DPA**) is entered into between Cloudnexa and the Customer and is incorporated into and governed by the terms of the cloud service provider agreement (**Agreement**) between the parties.

DEFINITIONS. Any capitalised term not defined in this DPA will have the meaning given to it in the Agreement.

- **Affiliate** *means* any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party.

- **Controller** *means* the Customer, the entity which determines the purposes and means of the process of Personal Data.

- **Customer Data** *means* data, which may include personal data and the categories of data submitted, stored, sent or received via the Service by Customer, its Affiliates or end users.

- **Data Subject** has the same meaning as the Directive (as amended from time to time or replaced by subsequent legislation).

- **DPA** *means* this data processing addendum and its schedules (together).

- **Directive** *means* Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

- **GDPR** *means* 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 and repealing the Directive.

- **Model Contract Clauses** *means* the standard contractual clauses for personal data transfer from controllers to processors c2010-593 - Decision 2010/87EU set out in **Schedule 3** of this DPA.

- **Personal Data** has the same meaning as in the Directive (as amended from time to time or replaced by subsequent legislation).

- **Processor** *means* Cloudnexa, Inc., the entity which Processes Personal Data on behalf of Controller.

- **Sub-processors** *mean* any person or entity engaged by Cloudnexa or an Affiliate to process Personal Data in the provision of the Services to Customer.

- **Services** *means* Cloudnexa subscription services.

1. PURPOSE.

Cloudnexa has agreed to provide the Services to the Customer in accordance with the terms of the Agreement. In providing the Services, Cloudnexa will process Customer Data on behalf of the Customer. Customer Data may include Personal Data. Cloudnexa will process and protect such Personal Data in accordance with the terms of this DPA. With respect to Customer Data, the parties

agree that Customer is the data controller and Cloudnexa is the data processor. Customer will comply with its obligations as a controller and Cloudnexa will comply with its obligations as a processor under the DPA. Where a Customer Affiliate is the controller with respect to certain Customer Data, Customer represents and warrants to Cloudnexa that it is authorized to instruct Cloudnexa and otherwise act on behalf of such Customer Affiliate in relation to the Customer Data in accordance with the DPA.

2. SCOPE.

In providing the Services to the Customer pursuant to the terms of the Agreement, Cloudnexa will treat Personal Data as confidential and only process Personal Data on behalf of the Customer and to the extent necessary to provide Services in accordance with both the terms of the Agreement and the Customer's instructions documented in the Agreement and this DPA.

3. TERM.

This DPA will automatically terminate upon the termination of the Agreement.

4. CLOUDNEXA OBLIGATIONS.

Cloudnexa may collect, process or use Personal Data only within the scope of this DPA. Cloudnexa confirms it will only process Personal Data on behalf of the Customer and in accordance with Customer's documented instructions. Cloudnexa will inform the Customer, if in Cloudnexa's opinion, any of the instructions regarding the processing of Personal Data provided by the Customer, violate any applicable data protection laws.

Cloudnexa will ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by terms materially no less restrictive than the terms of this DPA.

Cloudnexa shall maintain appropriate managerial, operational, and technical safeguards designed to preserve the integrity and security of Customer Data while in its possession and control hereunder, while taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Cloudnexa shall maintain appropriate measures to ensure a level of security appropriate to the risk, including but not limited to: (i) encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity and availability of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account will be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. Cloudnexa shall comply with the data protection and data security policies as set forth in **Schedule 2**.

Customer agrees that, in the course of providing the Services to the Customer, it may be necessary for Cloudnexa to access the Personal Data to respond to any technical problems, Customer queries, security monitoring, and to ensure the proper working of the Services. All such access by Cloudnexa will be limited to those purposes and performed by authorized personnel.

Where Personal Data relating to an EU Data Subject is transferred outside of the European Economic Area (EEA) it will be processed in accordance with the provisions of the Model Contractual Clauses, unless the processing takes place: (i) in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) by an organisation located in a country which has other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

Taking into account the nature of the processing and the information available to Cloudnexa, Cloudnexa will assist the Customer by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights and the Customer's compliance with the Customer's data protection obligations in respect of the processing of Personal Data.

5. CUSTOMER OBLIGATIONS

The Customer represents and warrants, in its use of the Services, that it will comply with the terms of the Agreement, this DPA and all applicable data protection laws.

The Customer represents and warrants that, as having sole responsibility for the Customer Data quality, legality and accuracy, has obtained any and all necessary permissions and authorizations necessary to permit Cloudnexa, its Affiliates and Sub-Processors, to execute their rights or perform their obligations under this DPA.

The Customer is responsible for compliance with all applicable data protection legislation, including requirements with regards to the transfer of Personal Data under this DPA and the Agreement. All Affiliates of the Customer who use the Services will comply with the obligations of the Customer set out in this DPA.

The Customer will implement appropriate technical, managerial and organisational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Customer will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security account will be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

Customer shall be responsible for the security of its administrative users' accounts and passwords and shall notify Cloudnexa immediately of any unauthorized use of any password or account or any other known or suspected breach of security. Customer shall be responsible for the acts or omissions of its administrative users in connection with the use of, and access to, the Service.

The Customer will take steps to ensure that any natural person acting under the authority of the Customer who has access to Personal Data only processes the Personal Data on the documented instructions of Customer.

The Customer acknowledges and agrees that some instructions from the Customer, including assisting with audits, inspections or DPIAs (defined below) by Cloudnexa, may result in additional fees. Cloudnexa will notify the Customer in advance of its fees for providing such assistance in advance.

6. NOTIFICATION OF SECURITY BREACH.

Cloudnexa will notify the Customer without undue delay after becoming aware of (and in any event within 72 hours of discovering) any confirmed accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to Customer's Personal Data (Data Breach).

Cloudnexa will take all commercially reasonable measures to secure the Personal Data, to eliminate the Data Breach, and to assist the Customer in meeting the Customer's obligations under applicable law. In the event of a security breach, Cloudnexa's System Administration Team and Security Team will perform a risk-based assessment of the situation and develop appropriate strategies in accordance with Cloudnexa incident response procedures, which include contacting the Customer and to contact Customer's primary (technical or business) point of contact or Security Operation Center (**SOC**) to brief them on the situation and provide resolution status updates.

7. AUDIT

Cloudnexa will make available to the Customer all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

Any audit conducted under this DPA will consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Customer, the Customer may conduct a more extensive audit which will be: (i) at the Customer's expense; (ii) limited in scope to matters specific to the Customer and agreed in advance; (iii) carried out during business hours and upon reasonable notice which must be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with Cloudnexa's day-to-day business. This clause does not modify or limit the rights of audit of the Customer, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

8. COMPLIANCE, COOPERATION AND RESPONSE.

Cloudnexa shall, to the extent legally permitted, promptly notify Customer if Cloudnexa receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, erasure, data portability, object to the processing (**Data Subject Request**). Taking into account the nature of the processing, Cloudnexa shall assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under data protection laws. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Cloudnexa shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Cloudnexa is legally permitted to do so and the response to such Data Subject Request is required under data protection laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Cloudnexa's provision of such assistance.

Cloudnexa will notify the Customer promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Customer, unless such notification is not permitted under applicable law or a relevant court order.

Cloudnexa may make copies of or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.

Cloudnexa will reasonably assist the Customer in meeting its obligation to carry out Data Protection Impact Assessments (**DPIA**), taking into account the nature of processing and the information available to Cloudnexa.

Cloudnexa will respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the parties agree that amendments are required, but Cloudnexa is unable to accommodate the necessary changes, the Customer may terminate the parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services will remain unaffected.

The Customer and Cloudnexa and, where applicable, their representatives, will cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA.

9. SUB-PROCESSORS.

The Customer agrees that: (i) Affiliates of Cloudnexa may be used as Sub-processors; and (ii) Cloudnexa and its Affiliates respectively may engage Sub-processors in connection with the provision of the Services.

All Sub-processors who process Personal Data in the provision of the Services to the Customer will comply with the obligations of Cloudnexa set out in this DPA.

Where Sub-processors are located outside of the EEA, Cloudnexa confirms that such Sub-processors: (i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) have entered into Model Contractual Clauses with Cloudnexa; or (iii) have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

Cloudnexa will make available to the Customer the current list of Sub-processors upon request which will include the identities of Sub-processors and their country of location. During the term of this DPA, Cloudnexa will provide the Customer with prior notification, via email, of any changes to the list of Sub-processors who may process Personal Data before authorising any new or replacement Sub-processors to process Personal Data in connection with the provision of the Services.

The Customer may object to the use of a new or replacement Sub-processor, by notifying Cloudnexa promptly in writing within 10 business days after receipt of Cloudnexa's notice. If the Customer objects to a new or replacement Sub-processor, and that objection is not unreasonable, the Customer may terminate the Agreement or applicable order with respect to those Services which cannot be provided by Cloudnexa without the use of the new or replacement Sub-processor. Cloudnexa will refund the Customer any prepaid and unused fees covering the remainder of the term of the applicable order following the effective date of termination with respect to such terminated Services.

10. LIABILITY

The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA. The parties agree that Cloudnexa will be liable for any breaches of this DPA caused by the acts and omissions of its Sub-processors to the same extent Cloudnexa would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

The parties agree that the Customer will be liable for any breaches of this DPA caused by the acts and omissions of its Affiliates as if such acts, omissions had been committed by Customer itself. Customer is not entitled to recover more than once in respect of the same claim.

11. GENERAL.

This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions will be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and will replace the invalid provision. The same will apply to any omissions.

To the extent of any conflict or inconsistency between the terms of this DPA and the remainder of the Agreement with respect to the privacy and security of Customer Data, the terms more protective of the Customer Data will apply. In all other cases, the terms of the Agreement control. Subject to the amendments in this DPA, the Agreement remains in full force and effect.

Customer may send any questions or concerns regarding this DPA to: privacy@Cloudnexa.com

_____/Customer	**Cloudnexa, Inc.**
Name:	Name:
Title:	Title:
Date:	Date:

SCHEDULE 1

This Appendix forms part of the Clauses.

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 the Customer and its end users.

Data importer
The data importer is Cloudnexa, Inc., a provider of a software service.

Categories of Data

The personal data transferred concern the following categories of data:

Data Subjects:

The personal data transferred concern the following categories of data subjects (please specify):

Processing Operations:

With respect to Customer's data, the parties acknowledge and agree that Customer is the 'data controller' (as defined in the Data Protection Legislation) and Cloudnexa is a 'data processor' (as defined in the Data Protection Legislation). Customer will comply with its obligations as a 'data controller' and Cloudnexa will comply with its obligations as a 'data processor' under the agreement.

Cloudnexa will process Customer data in accordance with Customer's written instructions and under this document.

Cloudnexa will only process Customer data in accordance with the agreement between the parties.

SCHEDULE 2

This Appendix forms part of the Clauses.

Cloudnexa shall have in place security safeguards that are designed to conform to or exceed industry best practices regarding the protection of the confidentiality, integrity and availability of customer data. These information security safeguards shall be materially consistent with, or more stringent than, the safeguards described in this Schedule.

Cloudnexa shall have in place security safeguards that are designed to conform to or exceed industry best practices regarding the protection of the confidentiality, integrity and availability of customer data. These information security safeguards shall be materially consistent with, or more stringent than, the safeguards described in this Schedule.

Cloudnexa's information security safeguards are consistent with Federal and State Laws and industry best practices to protect the confidentiality, integrity, and availability of customer data. Cloudnexa uses a defense-in-depth strategy to ensure the security of customer data. This is achieved by utilizing the National Institute of Standards and Technology (NIST) Risk Management Framework 800-37 as the foundation of our information security program. Cloudnexa is SSAE-16 SOC 2 Type II compliant and undergoes annual SOC 2 audits to verify that its information security practices, policies, procedures and operations meet or exceeds the rigorous SOC 2 standards for security, availability, confidentiality and processing integrity.

Cloudnexa employs role-based access controls to servers containing customer information which are consistent with job duties and contractual requirements. Access to customer information is limited to authorized company employees having a "need to know." Authorized employees must use individual account and multi-factor authentication to gain access to customer information. Authorization is done on a "least privilege" model.

Cloudnexa stores customer data on Cloudnexa servers housed within independently verified SSAE-16/SOC 1 Type II, ISO 27001, PCI certified authorized data centers (including Amazon Web Services AWS and Microsoft Azure Cloud Computing facilities). The data centers' physical and environmental security includes industry-leading network hardening and active monitoring, digital security video surveillance and 24/365 on-site security staff. Cloudnexa encrypts customer data at rest with FIPS 140-2 approved algorithms (AES-256).

Cloudnexa utilizes HTTPS for securing data in transit and web server to web browser communications. When a user accesses the web interface via an internet browser, the HTTP session is redirected to HTTPS protocol using a Transport Layer Security (TLS 1.1 and 1.2) or higher connection.

Cloudnexa's systems and networks are constantly monitored for security incidents, system health, network and traffic anomalies, and availability. Cloudnexa performs periodic internal web application vulnerability assessments to ensure application security controls are properly applied and operating effectively as designed. On at least an annual basis, Cloudnexa performs external vulnerability assessments using third-party web application and pen testing assessors. The scope of these external audits assesses compliance with the Open Web Application Security Project (OWASP) Top 10 Web Vulnerabilities. Vulnerability assessment results are incorporated into the Cloudnexa Software Development Lifecycle (SDLC) to remediate vulnerabilities and internally tracked through resolution.

Cloudnexa has a dedicated experienced security team with certifications that include:

Schedule 3

Model Contract Clauses

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)
FOR 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.

_____, (the data **exporter**)

and

Cloudnexa, Inc., (the data **importer**)

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

HAVE AGREED on the following Model 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 **Schedule 1 of the DPA.**

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 **Schedule 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 **Schedule 2** to this contract;

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

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

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

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

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of **Schedule 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 **Schedule 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 **Schedule 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 of by operation of law, in which case the data subject can enforce its rights against such entity.

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

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

Clause 7 ***Mediation and jurisdiction***

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

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

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

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

Clause 8 ***Cooperation with supervisory authorities***

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

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same

conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

Clause 9 ***Governing Law***

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

Clause 10 ***Variation of the contract***

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

Clause 11 **Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. 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.