DATA PROCESSING ADDENDUM ('DPA')

This Data Processing Addendum ("DPA") is entered into between Forest Admin, Inc., a company incorporated in Delaware, and its worldwide affiliates and subsidiaries (collectively, the "Provider" or "Forest Admin"), and the entity identified as the customer on the signature page of this Addendum ("Customer"). Forest Admin and Customer may each be referred to as a "Party" and collectively referred to as the "Parties".

This DPA shall be effective on the date it has been fully executed by the Parties and if it has been provided to Forest Admin in accordance with the instructions below (the "DPA Effective Date"). As of the DPA Effective Date, this DPA shall be incorporated by reference into the agreement between Customer and Forest Admin that governs Customer's use of the Service, whether such agreement is online or in a written agreement executed in counterparts with Forest Admin ("Agreement"). All capitalized terms used in this DPA but not defined shall have the meaning set forth in the Agreement. To the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern. This DPA replaces in its entirety any previously applicable DPA entered into or agreed upon by the parties prior to the DPA Effective Date.

This DPA sets out the terms that apply when Personal Data is Processed by Forest Admin under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with Data Protection Laws and respects the rights of Data Subjects whose Personal Data are Processed under the Agreement.

HOW TO EXECUTE THIS DPA

This DPA and the SSCs attached as Exhibit A (including Annex I, II and III) have been pre-signed by Forest Admin. When Forest Admin receives the completed and signed DPA and SSCs as specified below, this DPA and the SCCs will become a legally binding addendum to the Agreement. To make this DPA and the SCCs a part of the Agreement, Customer must:

1. Complete the information in the signature blocks on page 7 of this DPA.
2. Complete the information as Data Exporter on Pages 17.
3. Submit the completed and signed DPA and the completed and signed SCCs in Exhibit A (including Annex I, II and III) via email to: privacy@forestadmin.com

1. DATA PROCESSING

1.1 **Scope.** This DPA applies when Forest Admin Processes Customer Personal Data in providing the Services under the Agreement to Customer.

1.2 **Roles of the Parties.** The Parties agree that Forest Admin is a Processor with respect to its Processing of Customer Personal Data in providing the Services. Forest Admin will only Process Customer Personal Data in accordance with the Agreement, this DPA (including Appendix A), and the Orders (the "Documented Instructions"). Forest Admin will promptly inform Customer if it becomes aware that the Documented Instructions violate Data Protection Laws.

1.3 **Customer Obligations.** Customer is responsible for ensuring that no special categories of Personal Data (under GDPR Article 9), Personal Data relating to criminal convictions and offenses (under GDPR Article 10), or similarly sensitive Personal Data (defined in Data Protection Laws) is submitted to Forest Admin for Processing.

1.4 **Compliance with Laws.** Each Party will comply with all the Data Protection Laws applicable to its performance under this DPA.

2. DURATION

This DPA remains in effect until the later of (a) the expiration or termination of the Agreement, and (b) the return or deletion of Customer Personal Data in accordance with Section 6.

3. SECURITY AND CONFIDENTIALITY

Forest Admin will implement and maintain the technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, and unauthorized disclosure or access, as described in Appendix A – Annex 2 (the "**Technical and Organizational Measures**"). Forest Admin will take appropriate steps to ensure compliance with the Technical and Organizational Measures by its employees, agents, contractors, and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to Process Customer Personal Data have agreed to appropriate confidentiality obligations.

4. SUBPROCESSORS

4.1 **Subprocessor Authorization.** Customer generally authorizes Forest Admin to engage Subprocessors in accordance with this Section 4 and approves Forest Admin's use of the Subprocessors listed in the Subprocessors List. Forest Admin will update the Subprocessors List at least 30 days before appointing a new Subprocessor and will provide Customer with a mechanism to receive notifications of updates to the Subprocessors List (a "**Change Notice**"), which today is available through the Subprocessors List.

4.2 **Objections to Subprocessors.** Customer may object to the new Subprocessor on reasonable grounds related to the protection of Customer Personal Data by sending an email to privacy@forestadmin.com describing its legitimate, good-faith objection within 10 days of a Change Notice (an "**Objection Notice**"), in which case Forest Admin may satisfy the objection by (a) not using the Subprocessor to Process Customer Personal Data; (b) taking corrective steps requested by Customer in its Objection Notice; or (c) ceasing to provide the parts of the Services that involve the Subprocessor Processing Customer Personal Data, subject to a mutual agreement of the Parties. If none of the options outlined above are reasonably available and Customer's objection has not been resolved to the Parties' mutual satisfaction within 30 days of Forest Admin's receipt of the Objection Notice, either Party may terminate the affected Order and Forest Admin will refund to Customer a pro rata share of any unused amounts prepaid by Customer under the applicable Order for the Services on the basis of the remaining portion of the current terms of the Order. If Customer does not provide a timely Objection Notice with respect to a new Subprocessor, Customer will be deemed to have authorized Forest Admin's use of the Subprocessor and to have waived its right to object.

4.3 **Subprocessor Requirements.** Forest Admin will enter into a written agreement with each Subprocessor that contains data protection obligations equivalent to those in this DPA. Forest Admin will be liable for the actions and omissions of its Subprocessors undertaken in connection with Forest Admin's performance under this DPA to the same extent Forest Admin would be liable if performing the Services directly.

5. DATA SUBJECT REQUESTS

If Forest Admin receives a Data Subject Request, Forest Admin will (a) advise the Data Subject to submit the request to Customer directly, and (b) promptly notify Customer of the request. Where required by Data Protection Laws, Forest Admin will, on Customer's request and taking into account the nature of Customer Personal Data Processed, provide reasonable assistance to Customer in fulfilling the Data Subject Request to the extent Customer is unable through its use of the Services to address a particular Data Subject Request on its own. To the extent permitted by Applicable Law, Customer will be responsible for any costs arising from Forest Admin's assistance.

6. DATA DELETION

Commencing 30 days after the effective date of termination of the Agreement, Forest Admin will initiate a process on Customer's written request that deletes Customer Personal Data retained within 90 days. Notwithstanding the foregoing, to the extent Forest Admin is required by Applicable Laws to retain some or all Customer Personal Data, Forest Admin will not be obligated to delete the retained Customer Personal Data, and this DPA will continue to apply to the retained Customer Personal Data. Customer acknowledges that it is responsible for exporting any Customer Personal Data that Customer wants to retain prior to expiration of the referenced 30-day period pursuant to the Agreement.

7. PERSONAL DATA BREACHES

7.1 **Breach Notification.** Forest Admin will notify Customer without undue delay after becoming aware of a Personal Data Breach. Forest Admin's notification to Customer will describe (a) the nature of the Personal Data Breach, including, if known, the categories and approximate number of Data Subjects and Personal Data records concerned; (b) the measures Forest Admin has taken, or plans to take, to respond to and mitigate the Personal Data Breach; (c) any measures Forest Admin recommends that Customer take to address the Personal Data Breach; and (d) information related to Forest Admin's point of contact with respect to the Personal Data Breach. If Forest Admin cannot provide all the information above in the initial notification, Forest Admin will provide the information to Customer as soon as it is available.

7.2 **Breach Response.** Forest Admin will promptly take all actions relating to its Technical and Organizational Measures that it deems necessary and advisable to identify and remediate the cause of a Personal Data Breach.

7.3 **General.** Forest Admin's notification of or response to a Personal Data Breach will not constitute an acknowledgment of fault or liability with respect to the Personal Data Breach. The obligations in this Section 7 do not apply to Personal Data Breaches that are caused by Customer, Authorized Users, or providers of Customer Components. Except as may otherwise be required by Applicable Law (including any mandated deadlines under Data Protection Laws), if Customer decides to notify a Supervisory Authority, Data Subjects, or the public of a Personal Data Breach, Customer will make reasonable efforts to provide Forest Admin with advance copies of the notice(s) and allow Forest Admin an opportunity to provide any clarifications or corrections to them.

8. AUDITS

8.1 **Forest Admin's Audit Reports.** On Customer's request, and subject to the confidentiality provisions of the Agreement, Forest Admin will make available to Customer copies of, or extracts from, Forest Admin's audit reports related to the security of the Services, including, for example, its latest Penetration Testing Certificate.

8.2 **Customer's Audit Rights.** Customer may request (directly or through a third-party auditor subject to written confidentiality obligations) an audit of Forest Admin to verify Forest Admin's compliance with the terms of this DPA if such an audit is required by Data Protection Laws and Forest Admin's compliance cannot be demonstrated by means that are less burdensome on Forest Admin (including under Section 8.1). Any audit under this section must meet the following requirements: (a) Customer must provide Forest Admin at least 30 days' prior written notice of a proposed audit unless otherwise required by a competent supervisory authority or Data Protection Laws; (b) Customer may not perform more than one audit in any 12-month period, except where required by a competent supervisory authority; (c) Customer and Forest Admin must mutually agree on the time, scope, and duration of the audit in advance; (d) Customer must reimburse Forest Admin for its time expended in connection with an audit at Forest Admin's reasonable professional service rates, which will be made available to Customer on request; (e) Customer must ensure that its representatives performing an audit protect the confidentiality of all information obtained through the audit in accordance with the Agreement, execute an enhanced mutually agreeable nondisclosure agreement if requested by Forest Admin, and abide by Forest Admin's security policies while on Forest Admin's premises; and (f) Customer must promptly disclose to Forest Admin any written audit report created, and any findings of noncompliance discovered, as a result of the audit.

9. IMPACT ASSESSMENTS AND PRIOR CONSULTATION

Taking into account the nature of the Processing and the information available to Forest Admin, Forest Admin will, when required by Data Protection Laws, assist Customer with its obligations related to data protection impact assessments (where related to the Services, and only to the extent that Customer does not otherwise have access to the relevant information) and prior consultation with supervisory authorities, including by providing the information outlined in Section 8.1 above.

10. DATA TRANSFERS

To protect transfers of Personal Data out of the EEA, Switzerland, and the UK, the Parties agree to enter into the SCCs and the UK Transfer Addendum as described below.

10.1 **Transfers from the EEA.** Where a Restricted Transfer is made from the EEA, the SCCs attached in Exhibit A are incorporated into this DPA and apply to the transfer.

10.2 **Transfers from Switzerland.** Where a Restricted Transfer is made from Switzerland, the SCCs attached in Exhibit A are incorporated into this DPA and apply to the transfer, except that:

10.2.1 in Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner if the Restricted Transfer is governed by the Swiss Federal Act on Data Protection;

10.2.2 references to "Member State" in the SCCs refer to Switzerland, and data subjects located in Switzerland may exercise and enforce their rights under the SCCs in Switzerland; and

10.2.3 references to the "General Data Protection Regulation," "Regulation 2016/679," and "GDPR" in the SCCs refer to the Swiss Federal Act on Data Protection (as amended or replaced).

10.3 **Transfers from the UK.** Where a Restricted Transfer is made from the UK, the UK Transfer Addendum is incorporated into this DPA and applies to the transfer. The UK Transfer Addendum is completed with the information in Exhibit A and Annex 1, 2, and 3; and both "Importer" and "Exporter" are selected in Table 4.

10.4 **Specific application of the SCCs.** The following terms apply to the SCCs:

10.4.1 Customer may exercise its audit rights under the SCCs as set out in Section 8 above.

10.4.2 Forest Admin may appoint Subprocessors under the SCCs as set out in Section 4 above.

10.4.3 With respect to Restricted Transfers made to Forest Admin, Forest Admin may neither participate in, nor permit any Subprocessor to participate in, any further Restricted Transfer unless the further Restricted Transfer is made in full compliance with Data Protection Laws and in accordance with applicable SCCs or an alternative legally compliant transfer mechanism.

10.4.4 If any provision of this Section 10 is inconsistent with any terms in the SCCs, the SCCs will prevail.

11. LIMITATION OF LIABILITY

Each Party's liability taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability provisions of the Agreement.

12. CONFLICT

In the event of a conflict or inconsistency between the Agreement, this DPA, and the SCCs, the terms of the following documents will prevail (in order of precedence): the SCCs; then this DPA; and then the Agreement.

13. MODIFICATIONS

Forest Admin may make changes to this DPA where (a) the change is required to comply with an Applicable Law; or (b) the change is commercially reasonable, does not materially reduce the security of the Services, does not change the scope of Forest Admin's processing of Customer Personal Data, and does not have a material adverse impact on Customer's rights under this DPA.

14. DEFINITIONS

Capitalized terms not otherwise defined in this DPA or the Agreement have the meanings assigned to them below.

“Controller” means the entity that determines the purposes and means of Processing Personal Data.

“Customer Data” means data from Customer’s Environment that are submitted for Processing by the Services. Through Customer’s configuration and use of the Services, Customer has control over the types and amounts of Customer Data.

“Customer Personal Data” means Customer Data comprising Personal Data.

“Data Protection Laws” means data protection or privacy laws and regulations directly applicable to a Party’s Processing of Personal Data under the Agreement, including European Data Protection Laws.

“Data Subject” means the identified or identifiable natural person to whom Personal Data relates.

“Data Subject Request” means a request from a Data Subject exercising his or her rights under Data Protection Laws that relates to Customer Personal Data and identifies Customer.

“**EEA**" means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein, as well as, for the purposes of this DPA, Switzerland and the United Kingdom.

“European Data Protection Laws” means the GDPR; the UK GDPR; and any national data protection laws, implementing regulations, or binding decisions made under the GDPR or the UK GDPR.

“GDPR” means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing of Directive 95/46/EC.

“Personal Data” means any information relating to an identified or identifiable natural person.

“Personal Data Breach” means a breach of Forest Admin’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

“Process” and “Processing” mean any operation or set of operations which is performed on Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

“Processor” means the entity that Processes Personal Data on behalf of a Controller.

“Restricted Transfer” means (i) where the GDPR applies, a transfer of Customer Personal Data or Account Data from the EEA to a country outside of the EEA that is not subject to an adequacy determination by the European Commission; (ii) where the Swiss Federal Act on Data Protection applies, a transfer of Customer Personal Data or Account Data from Switzerland to a country that is not subject to an adequacy determination by the Swiss Federal Data Protection and Information Commissioner; and (iii) where the UK GDPR applies, a transfer of Customer Personal Data or Account Data from the UK to a country that is not the subject of adequacy regulations under section 17A of the United Kingdom Data Protection Act of 2018.

“SCCs” means the standard contractual clauses for international transfers annexed to the European Commission’s commission implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, published on June 4, 2021, including as incorporated into the UK Transfer Addendum, if applicable.

“Subprocessor” means any Processor engaged by Forest Admin to Process Customer Personal Data on Forest Admin’s behalf while providing the Services.

“Subprocessors List” means the list of Subprocessors available at https://www.forestadmin.com/sub-processors.

“UK” means the United Kingdom.

“UK GDPR” means the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom’s European Union (Withdrawal) Act 2018.

“UK Transfer Addendum” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, published by the UK Information Commissioner’s Office on March 21, 2022.

[Signature page follows.]

Signature

Both Parties hereby acknowledge they have fully read and understood the terms of this Agreement. This Agreement may be executed by facsimile or by other means of electronic transmission and in two or more counterparts, each of which shall be deemed an original and all of which together shall constitute one instrument.

CUSTOMER:	PROVIDER: FOREST ADMIN, INC.
Authorized Signature:	Authorized Signature: DocuSigned by: Sandro Munda 5F59F9D2E5DF4BB...
Print Name and Title:	Print Name and Title: Sandro Munda, CEO
Signed on:	Signed on: 22-Dec-2023
Address:	Address: 490 Post Street, Suite 640 San Francisco, CA 94102
Email address:	Email address: privacy@forestadmin.com

Exhibit A - STANDARD CONTRACTUAL CLAUSES

TRANSFER CONTROLLER TO PROCESSOR

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

---

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these

Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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.

(f) 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.

(g) 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.

(h) 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.

(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

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

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

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

behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

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

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

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

Clause 13

Supervision

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

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(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

15.1 Notification

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

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

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

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

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the

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

requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of Paris, France.

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

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

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Processing Customer Personal Data for the purpose of providing, supporting, and improving the Services.

Signature and date:

Role (controller/processor): controller

Data importer(s):

1. Name: Forest Admin, Inc.

Address: 490 Post Street, Suite 640, San Francisco, CA 94102 (United States)

Contact person's name, position and contact details: Sandro Munda, CEO, dpo@forestadmin.com

Activities relevant to the data transferred under these Clauses: Processing Customer Personal Data for the purpose of providing, supporting, and improving the Services.

Signature and date: 22-Dec-2023

Role (controller/processor): processor

DocuSigned by:
Sandro Munda
5F59F9D2E5DF4BB...

2. Name: Forest Admin France

Address: 5 rue Cadet, 75009 Paris (France)

Contact person's name, position and contact details: Sandro Munda, Président, dpo@forestadmin.com

Activities relevant to the data transferred under these Clauses: Processing Customer Personal Data for the purpose of providing, supporting, and improving the Services.

Signature and date: 22-Dec-2023

Role (controller/processor): processor

DocuSigned by:
Sandro Munda
5F59F9D2E5DF4BB...

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

- Authorised Users;
- employees of Customer;
- consultants of Customer;
- contractors of Customer;
- agents of Customer; and/or
- third parties with which Customer conducts business.

Categories of personal data transferred

Customer Personal Data that is sent to Forest Admin by Customer for the purpose of using the Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data is transferred.

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

Frequency of the transfer is controlled by Customer and is tied to the usage of the Service by Customer.

Nature of the processing

Analysis, storage, and other Services as described in the Agreement, Order(s), DPA, and Documentation.

Purpose(s) of the data transfer and further processing

Customer Personal Data transferred will be processed in accordance with the Agreement, the Terms and Conditions and any Order Form and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain and update the Services provided to Customer;
- to provide customer and technical support to Customer; and
- disclosures in accordance with the Agreement, as compelled by law.

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

Customer Personal Data is retained in accordance with the terms set out in clause 6 of the DPA.

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

The subject matter of Personal Data transferred to Subprocessors is Customer Personal Data, which is transferred to Subprocessors to provide, support, and improve the Services, as outlined in the agreements between Customer and Forest Admin.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is determined in accordance with data protection or privacy laws and regulations directly applicable to a Party's Processing of Personal Data under the Agreement, including European Data Protection Laws.

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

As of the date of this DPA, Provider's technical and organizational measures include the following:

Category	**Sub-category**	**Measures**
Organization of Information Security	Segregation of duties	Provider shall ensure that conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the assets supporting the Service delivered.
Human resource security	Screening	When allowed by law, Provider shall systematically perform, or engage a third-party screening company to do, background checks on employees or third parties working on the contract, including but not limited to the following checks: - Person's identity and address - Academic qualifications - Work experience
	Terms and conditions of employment	Provider shall systematically include in the contract of employment of his employees: - Unauthorized Disclosure of Sensitive Information - Data Protection legislation
	Management responsibilities	Provider's staff shall periodically receive security training. Provider's management must ensure that employees and contractors: - are aware of and understand their information security roles and responsibilities prior to being granted access to confidential information or information systems - are provided with information security expectations associated with their role within the organization and related to Customer
Asset Management	Acceptable use of assets	Provider shall develop, implement and maintain a comprehensive Acceptable Use Policy for its Information Assets.
	Handling of assets	Without prejudice to Provider's obligations, Provider shall (and shall procure that its sub-contractors shall) in accordance with Good Industry Practice protect against corruption, loss or disclosure all Customer's confidential information.
Logical Security / Access	Access control policy	Provider shall properly manage Access control, including the following topics: - Policy on the use of network services - User registration and de-registration - User Access Provisioning - Management of privileged access rights - Management of secret authentication information on users - Review of user access rights - Removal or adjustment of access rights - Use of secret authentication information - Information access restriction - Secure log-on procedures - Password management system - Use of privileged utility programs - Access control to program source code
Physical and environmental security	Physical security perimeter	Provider shall properly manage security policy, including the following topics: - Physical security perimeter

		- Securing office, room and facilities - Equipment siting and protection - Security disposal or re-use of equipment - Unattended user equipment
Operations Security	Documented operating procedures	Provider shall develop, implement and maintain comprehensive operating processes for the Services provided and underlying IT, including the following topics: - Change management, including emergency changes - Separation of development, test and operational environments - Controls against malware - Information backup - Event logging - Protection of log information - Installation of software on operational systems - Management of technical vulnerabilities and patching
	Security requirements analysis and specification	Provider shall ensure that development activities are carried out in accordance with a documented system development methodology. This methodology shall consider OWASP recommendations for Web application development or other secure development methodologies suitable for the development environment. (in e.g. SecDevOps). The following topics shall be addressed: - Security requirements analysis and specification - Securing applications services on public networks - Protecting application services transactions - Secure development policy - Outsourced development - System security testing - System acceptance testing - Protection of test data
Communications Security	Network controls	Provider shall ensure that its network is designed and implemented so as to be able to cope with current and predicted levels of traffic and shall be protected using all available in-built security controls. Topics to be addressed are: - Network controls - Security of network services - Segregation in networks - Information transfer policies and procedures - Agreements on information transfer
	Electronic messaging	Provider shall ensure that its electronic messaging systems (in e.g. mail, instant messaging) are protected by a combination of policy (including a usage policy), training and documented procedural and technical security controls.
Supplier Relationships	Information security policy for supplier relationships	Provider shall ensure that services required to support the Services provided to the Customer shall be obtained from service providers capable of providing security controls no less rigorous than those that the Service Provider is required to comply with pursuant to this Schedule. When possible, such services shall be provided under appropriate contracts. When available, Provider shall ensure that agreements with Sub-contractors include a right for the Provider to conduct a security review for the purposes of ensuring they are meeting the Provider's obligations under this Agreement. The results of any such security review shall be provided to the Customer promptly on request.

ANNEX III - LIST OF SUB-PROCESSORS

Annex III of the SCCs is completed with the information in the Subprocessors List.