DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

Forest Admin – 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 data processing agreement 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 Applicable Law and respects the rights of individuals whose Personal Data are Processed under the Agreement.

HOW TO EXECUTE THIS DPA

This DPA and the Standard Contractual Clauses attached as Exhibit A (including Appendices 1 & 2) have been pre-signed by Forest Admin. When Forest Admin receives the completed and signed DPA and Standard Contractual Clauses as specified below, this DPA and the Standard Contractual Clauses will become a legally binding addendum to the Agreement. To make this DPA and the Standard Contractual Clauses a part of the Agreement, Customer must:

1. Complete the information in the signature blocks on page 8 of this DPA.
2. Complete the information as Data Exporter on Pages 9, 17, 20 and 23.
3. Submit the completed and signed DPA and the completed and signed Standard Contractual Clauses (including Appendix 1 and 2) via email to: privacy@forestadmin.com

1. Definitions

"**Applicable Law(s)**" means all applicable laws, regulations, and other legal or regulatory requirements in any jurisdiction relating to privacy, data protection/security, or the Processing of Personal Data, including without limitation the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("CCPA") and the General Data Protection Regulation, Regulation (EU) 2016/679 ("GDPR"). For the avoidance of doubt, if Forest Admin's processing activities involving Personal Data

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

are not within the scope of an Applicable Law, such law is not applicable for purposes of this Addendum.

"**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.

"**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"**Personal Data**" means any Customer Content that includes "personal data," "personal information," and "personally identifiable information," and such terms shall have the same meaning as defined by Applicable Law.

"**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making such data available, alignment or combination, restriction, erasure or destruction.

"**Standard Contractual Clauses**" means the agreement by and between Forest Admin and Customer, attached hereto as Exhibit A, pursuant to the EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of Personal Data from the EEA to processors established in third countries under Directive 95/46/EC of the European Parliament and of the European Council, completed as described in the "Data Transfers" section below.

"**Sub-processor**" means any Forest Admin affiliate or party engaged by Forest Admin for the Processing of Personal Data in connection with the Service.

2. Details of processing of Customer Personal Data

2.1 The Provider is authorized to process on behalf of Customer the necessary personal data to provide the following services (the "Services"): providing Customer with an administrative web interface tool.

2.2 The nature of the operations performed on the data is identifying users invited by Customer (the "Users") to use the Services.

2.3 The purpose of the processing is to authenticate Users who can access the information registered in Customer's IT infrastructure.

2.4 The personal data processed are Users authentication and identification data (name, e-mail address, password).

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

2.5 The categories of persons concerned are the Users invited by Customer to use the Provider's Services.

2.6 For the execution of the Services, Customer provides the Provider with the Users' authentication and identification data (name, e-mail address, password).

3. Personal data protection

3.1 Each party undertake to comply with the applicable regulations on personal data processing, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which is applicable from 25 May 2018 (hereinafter "*the General Data Protection Regulation*").

3.2 The Provider is authorized to process, on behalf of Customer, the necessary Personal Data for purposes of providing the Services.

3.3 For the purposes of the Services provided by the Provider, the Parties agree that Customer acts as a Data Controller and that Provider acts as a Processor of Customer's Personal Data.

3.4 As the Data Processor, Provider undertakes to:

(i) process the data solely for the purpose(s) subject to the processing detailed in article 2;

(ii) process the data in accordance with the documented instructions from Customer appended hereto. Where the Provider considers that an instruction infringes the GDPR or of any other legal provision of the Union or of Member States bearing on data protection, it shall immediately inform Customer thereof. Moreover, where the Provider is obliged to transfer personal data to a third country or an international organization, under Union law or Member State law to which the Provider is subject, the Provider shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(iii) guarantee the confidentiality of personal data processed hereunder;

(iv) ensure that the persons authorized to process the personal data hereunder:
- have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,
- receive the appropriate personal data protection training;

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

(v) take into consideration, in terms of its tools, products, applications or services, the principles of data protection by design and by default;

(vi) Sub-processing:

i. Authorized Sub-processors; List; Liability: Customer acknowledges and agrees that Provider may retain certain third parties as Sub-processors to Process Personal Data on Provider's behalf in order to provide the Services. A list of Provider's third-party Sub-processors, which may be updated from time to time, is maintained at https://www.forestadmin.com/subcontractors/. Prior to a Sub-processor's Processing of Personal Data, Provider will impose contractual obligations on the Sub-processor substantially the same as those imposed on Provider under this DPA. Provider remains liable for its Sub-processors' performance under this DPA to the same extent Provider is liable for its own performance.

ii. Changes to Sub-processors: Provided that Customer signs up for notifications at https://forms.gle/TbPEK7Z66CzHTiYp8, Provider shall provide prior notice of any new third-party Sub-Processors. After being notified, Customer will have seven (7) business days to notify Provider in writing of any reasonable objection it has to the new third-party Sub-Processor(s). Failure to notify Provider within this time frame will be deemed approval of the new third-party Sub-Processor(s). In the event Customer provides reasonable objection, Provider will use reasonable efforts to make a change in the service or Customer's configuration available to avoid processing of Personal Data by such third-party Sub-Processor. If Provider is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, Customer may terminate the applicable order with respect to the affected service that cannot be provided without use of the rejected third-party Sub-Processor.

iii. Copies of Sub-processor Agreements Pursuant to the Standard Contractual Clauses: The parties agree that copies of the Sub-processor agreements that must be provided to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, redacted by Provider and that such copies will be provided by Provider only upon written request of Customer and in a manner determined by Provider.

(vii) Data Transfers: The Provider as well as any Sub-processor undertake not to transfer personal data outside the EEA without Customer's approval and on the terms that the Customer deems appropriate, unless they are required to do so under the law of the EEA or the law of the Member State of the EEA to which they are subject. In this case, the Provider or the Sub-processor informs the Data Controller of this legal obligation prior to the Processing, unless the right concerned prohibits such information for important reasons of public interest.

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

In the event that Customer accepts the transfer of data outside the EEA, the processing of the data in the context of the transfer must be framed by the appropriate guarantees provided by the European Data Protection Regulation in Articles 44 to 49, such as standard contractual data protection clauses adopted by the EU Commission or binding corporate rules.

Notwithstanding the above, Customer expressly accepts the transfer of data outside the EEA for purposes of their processing by the Sub-processors referred to in the list mentioned in article 3.4 (vi) that are established in the United States.

Customer declares to be informed and accepts that the Sub-processors have entered into a contract with the Provider that contain model clauses that have been approved by the EU Commission as set forth in Exhibit A or by another competent public authority in accordance with applicable data protection regulations.

(viii) Data subjects' right to information: It is the Customer's responsibility to inform the data subjects concerned by the processing operations at the time data are being collected.

(ix) Exercise of data subjects' rights: The Provider shall assist the Customer, insofar as this is possible, for the fulfilment of its obligation to respond to requests for exercising the data subject's rights: right of access, to rectification, erasure and to object, right to restriction of processing, right to data portability, right not to be subject to an automated individual decision (including profiling).

Where the data subjects submit requests to the Provider to exercise their rights, the Provider must forward these requests as soon as they are received by email to the email address provided in the signature block of this DPA.

(x) Notification of personal data breach: The Provider shall notify Customer of any personal data breach no later than 36 (thirty-six) hours after having become aware of it and by any written means including email. Said notification shall be sent along with any necessary documentation to enable Customer, where necessary, to notify this breach to the competent supervisory authority.

(xi) Assistance lent by the Provider to Customer regarding compliance with its obligations: The Provider shall assist Customer in carrying out data protection impact assessments, as well as with regard to prior consultation of the supervisory authority.

(xii) Security

i. Security Measures: Provider shall implement appropriate technical and organizational measures as required by Article 32 GDPR to protect Personal Data from Personal Data

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

Breaches and to preserve the security and confidentiality of the Personal Data, in accordance with Provider's security standards set forth in the attached Appendix 2.

ii. Provider's technical and organizational measures are subject to technical progress and further development. Accordingly, Provider reserves the right to modify the technical and organizational measures provided that the security of the Provider Services is not degraded.

(xiii) Fate of the data: At the end of the service bearing on the processing of such data, the Provider undertakes to, at the choice of Customer, destroy or return all personal data to Customer. Together with said return, all existing copies in the Provider's information systems must be destroyed.

(xiv) The Data Protection Officer: in accordance with Article 37 of the GDPR, the Provider has appointed a data protection officer, who can be contacted at the following address: dpo@forestadmin.com

(xv) Record of categories of processing activities: The Provider states that it maintains a written record of all categories of processing activities carried out on behalf of Customer.

(xvi) Audits: If and to the extent required by Applicable Law, Provider shall assist with audits of Provider, including inspections, conducted by Customer or another third-party representative mandated by Customer. Any such audits shall be subject to the following conditions: so long as the Agreement remains in effect and at Customer's sole expense, Customer may request that Provider provide it with documentation, data, and records ("Records") no more than once annually relating to Provider's compliance with this DPA (an "Audit"). To the extent Customer uses a third-party representative to conduct the Audit, Customer shall ensure that such third-party representative is bound by obligations of confidentiality no less protective than those contained in this Agreement. Customer shall provide Provider with fifteen (15) days prior written notice of its intention to conduct an Audit. Customer shall conduct its Audit in a manner that will result in minimal disruption to Provider's business operations. Customer shall not be entitled to receive data or information of other clients of Provider or any other Provider Confidential Information not directly relevant for the authorized purposes of the Audit. If any material non-compliance is identified by an Audit, Provider shall take prompt action to correct such non-compliance. For the avoidance of doubt, this provision does not grant Customer any right to conduct an on-site audit of Provider's premises. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with this Section.

3.5 As the Data Controller, Customer undertakes to:

(i) provide the Provider with the data mentioned in article 2 hereof;

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

(ii) document, in writing, any instruction bearing on the processing of data by the Provider;
(iii) ensure, before and throughout the processing, compliance with the obligations set out in the General Data Protection Regulation on the Provider's part;
(iv) supervise the processing, including by conducting audits and inspections with the Provider.

[Signature page follows.]

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

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: 17-Sep-2020
Address:	Address: 490 Post Street, Suite 640 San Francisco, CA 94102
Email address:	Email address: privacy@forestadmin.com

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

Exhibit A - STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: _____

Address: _____

e-mail: _____

hearafter the “data exporter”

And

Name of the data importing organisation: Forest Admin, Inc.

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

e-mail: privacy@forestadmin.com

hereafter the “data importer”

each a ‘party’; together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1 hereafter.

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

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 ([1]);

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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e	'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

f	'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 - Details of the transfer

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

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

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 sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

4.	The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

a	that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

b	that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;

c	that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

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 sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h	to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

	agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b	that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c	that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

d	that it will promptly notify the data exporter about:	
	i	any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
	ii	any accidental or unauthorised access; and
	iii	any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e	to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f	at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g	to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

	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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

i	that the processing services by the sub-processor will be carried out in accordance with Clause 11;

j	to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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.

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

Clause 11 - Sub-processing

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses [3]. Where the sub-processor 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 sub-processor's obligations under such agreement.

2.	The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3.	The provisions relating to data protection aspects for sub-processing 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 sub-processing 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 sub-processor 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.

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

2.	The data importer and the sub-processor 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.

On behalf of the data exporter:

Name: _____

Position: _____

Address: _____

	Signature :

On behalf of the data importer:

Name: Sandro Munda

Position: CEO

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

	Signature : DocuSigned by: Sandro Munda 5F59F9D2E5DF4BB...

(1) Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(2) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

([3]) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

Appendix 1 to the Standard Contractual Clauses

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

As per article 1 of the DPA:

Data exporter

Data Exporter is the legal entity identified as “Customer” in the DPA.

Data importer

The data importer is Forest Admin, Inc. which offers services aimed at providing administrative web interface and tools for companies.

Data subjects

The categories of persons concerned by the personal data transferred are the Users invited by Customer to use the Provider’s Services.

Categories of data

The personal data processed concern Users authentication and identification (name, e-mail address, password) data categories.

Special categories of data

Not applicable.

Processing operations

The objectives of the Processing of Personal Data by the data importer is the performance of the Services pursuant to the Agreement and in particular the authentication and identification of Users invited by Customer to use the Provider’s Services.

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

DATA EXPORTER

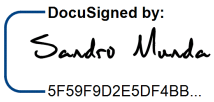
Name: _____

Authorised Signature :

DATA IMPORTER

Name: Sandro Munda

Authorised Signature :



DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

Appendix 2 to the Standard Contractual Clauses

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

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Provider undertakes to comply with the measures hereafter to ensure the security of the Personal Data processed on behalf of Customer:

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

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

		- 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

DocuSign Envelope ID: 231378AA-CF63-41D4-82A0-85853D2662BD

		- 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.

DATA EXPORTER

Name: _____

Authorised Signature :

DATA IMPORTER

Name: Sandro Munda

Authorised Signature : DocuSigned by: Sandro Munda 5F59F9D2E5DF4BB...