

Eddy HR, LLC EU Data Processing Agreement

DPA Background

This EU Data Processing Agreement (“DPA”) supplements our online Platform License and Terms of Service and Privacy Policy (together and individually, the “Agreement”) with clients (“Client” or “you”) insofar as they relate to processing of data subject to the European Union’s General Data Protection Regulation (“GDPR”). To the extent it conflicts with our Terms of Service or our Privacy Policy, this DPA will control. Capitalized terms used in this DPA shall have the same meaning set forth for those terms in the GDPR, unless a different meaning is specified herein.

Eddy HR, LLC (“Eddy,” “we,” or “us”) is a software as a service provider. As such, we act as a “Processor” under the GDPR. As one of our clients, you control the means and purposes for the processing of the data you gather using our services (the “Services”), and thus, you are a Controller under the GDPR. Unless otherwise agreed between us in writing, those items the GDPR requires of Processors will be our responsibility, and those items required of Controllers will be your responsibility. Specifically, the parties agree as follows:

How to Execute this DPA

We have adopted this DPA and made it effective through the Terms of Services into which our Clients enter with us. No further execution of the DPA is necessary by you or Eddy. That includes the signature lines showing in the Standard Contractual Clauses attached to this DPA. The Terms of Service incorporate both this DPA and the attached Standard Contractual Clauses, so no further signature of either document is required.

Our GDPR Obligations

When you use the Services, you may obtain Personal Data about your job applicants, prospects, employees, marketplace partners, customers, vendors, suppliers, or other individuals with whom you interact, or about whom you gather personal data (“Your Personal Data”), using the Services (collectively and individually, “Your Data Subjects”). That Personal Data may be subject to the protections of the GDPR. For purposes of clarity, the parties agree that Your Personal Data does not include data that is aggregated or anonymized in a manner that eliminates the likelihood that the data can be tracked or identified to any specific individual.

Each party agrees that it will act in full compliance with the requirements of the GDPR and agrees to indemnify, defend and hold harmless the other party from and against any losses, liabilities, damages, settlements, or other damages arising out of or relating to its own acts and omissions that do not comply with the requirements of the GDPR. This duty to indemnify, defend, and hold harmless includes fines that may be imposed by a governing authority and any and all reasonable attorneys’ fees and court costs.

Acknowledging that certain of your obligations as a Controller must be passed along to any company or individual that Processes the Personal Data of Your Data Subjects, we agree to

perform the following functions and to facilitate your compliance with the GDPR in the following ways:

1.1 Right of Access by Data Subject and Communication with Authorities and Your Data Subjects

We agree that, in order to assist you in your obligations as a Controller, we will implement the necessary technical and organizational measures to allow you to (1) respond to any request by any individual to exercise his or her rights under the GDPR, and (2) respond to correspondence, inquiries, or complaints from entitled third parties such as individuals, regulators, courts, and other authorities in connection with the processing of Personal Data. If any such requests or correspondence is received directly by us, we will forward you the request or correspondence and will wait for further direction from you before taking action. We will not communicate with authorities or Your Data Subjects without receiving your advance permission, except as required by applicable law. Upon documented request from you, we will correct, supplement, modify or delete any of Your Personal Data, except as required by applicable law.

1.2 Use Limitation

We agree that we will not use or process any of Your Personal Data for any purpose other than the purpose set forth in the Agreement, except to respond to document requests from you regarding Your Personal Data. In no event will we process, use, or transfer any of Your Personal Data for our own purposes or for the purposes of any third party. In addition, we will delete all Your Personal Data from our systems thirty (30) days after termination of the Agreement, except as may be required by applicable law. Certain of Your Personal Information is subject to the laws of various jurisdictions regarding archiving of employment-related data. To comply with that broad array of laws, and to allow us to facilitate the restarting of clients who may have terminated their agreement with us, we keep the employment-related data for a period of seven years, unless a client requests us to delete that data, in which case we will delete the data within thirty (30) days after receipt of the request. You also agree that you will not use or process any Personal data of any Data Subject for any purpose other than the purposes for which you have consent from the Data Subject.

1.3 Standard Contractual Clauses and International Transfers of Data

To the extent your transfer of Your Personal Data to us involves a transfer out of the EU, upon your entering into this DPA as provided above, we agree to comply with the Standard Contractual Clauses attached hereto as Exhibit A.

In the event of any conflict between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall control and supersede. If the European Union or courts thereof decide that the Standard Contractual Clauses are insufficient protection for citizens of the EU, then the parties agree to work in good faith together to determine how a new valid method can be implemented to meet any new requirements.

We agree that we will not process or transfer any of Your Personal Data originating from the European Economic Area in any country or territory that has been determined to offer an

inadequate level of data protection unless it has first obtained your consent or ensured that a valid transfer mechanism similar to, but not less restricting than the Standard Contractual Clauses is in place with respect to such country or territory.

1.4 Processing Confidentiality and Agreements by Agents

We agree that we will keep Your Personal Data strictly confidential and that we will ensure that any of our employees, vendors, or other agents “**Our Agents**” who have access to Your Personal Data (1) are informed of and subject to this strict duty of confidentiality; (2) access and process only such of Your Personal Data as is strictly to perform our obligations under the Agreement; and (3) agree not to permit any person to process Your Personal Data who is not subject to the foregoing duties. We accept responsibility for the conduct of Our Agents in this regard, including their acts, errors and omissions.

1.5 Disposition of Your Personal Data Upon Request or Termination

At your request or at termination of the Agreement, whichever is sooner, we agree to delete or return to you all Your Personal Data, including any of Your Personal Data subcontracted to a third party for processing, except as required by applicable law. At that time, with respect to Your Personal Data that we are required by applicable law to retain, we will isolate and protect Your Personal Data from further processing, except as required by applicable law. We will ensure that any of our subprocessors who are in possession of Your Personal Data shall also comply with this provision. Notwithstanding the foregoing, certain of Your Personal Information is subject to the laws of various jurisdictions regarding archiving of employment-related data. To comply with that broad array of laws, and to allow us to facilitate the restarting of clients who may have terminated their agreement with us, we keep the employment-related data for a period of seven years, unless a client requests us to delete that data.

1.6 Security Incidents and Security

We will at all times make commercially reasonable efforts to ensure that Your Personal Data is adequately protected in accordance with the requirements of the GDPR. To this end, we agree that we will implement appropriate technical and organizational measures to protect Your Personal Data from security incidents. These measures are described in Exhibit B to this DPA.

When we become aware of any security incident, which consists of the unpermitted, accidental, or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any of Your Personal Data, we will inform you without any undue delay, and in no event longer than 24 hours after we discover the security incident. We will cooperate reasonably with you and provide you the information you need in order to fulfill your data breach obligations under the GDPR. We will also take other further measures and actions that are necessary to remedy or mitigate the effects of the security incident, and we will keep you informed of every material development connected with the security incident. Except as required by law, we will not take action to notify Your Data Subjects of any security incident.

1.7 Subprocessors

In the course of providing our Services, we may be required to contract with a third-party processor (“**Subprocessor**”) to perform a portion of the Services. We have included as Exhibit C a list of the Subprocessors we currently use. We will not add any additional Subprocessors without informing you of such Subprocessors and giving you an opportunity to object to the use of such Subprocessors. We agree to impose the same data protection obligations upon each of our Subprocessors that we agree to in this DPA.

For the avoidance of doubt, the approval requirements as set out in this subsection will not apply in cases where we subcontract ancillary services to third parties without having access to Your Personal Data. Such ancillary services are not considered data processing.

1.8 Audits, Requests from Law Enforcement, and Impact Assessment

In certain instances, you as a Controller are required to submit to an audit to show that you are complying with the provisions of the GDPR. In any such instance, we agree to cooperate fully with such audit and to maintain a reasonable record of processing activities that we carry out on your behalf. After reasonable notice, we will allow you or your auditors to audit our compliance with this DPA, to include communication with our staff and access to our systems and information; provided you conduct your audit during normal business hours and make reasonable efforts to minimize the disruption to our business.

If we are requested by law enforcement to disclose any of Your Personal Data, we will, unless prohibited by law, inform you of the request, attempt to re-direct the law enforcement agency to contact you directly, and only provide such information as required by law.

In the event that you believe that our processing of Your Personal Data is likely to result in a high risk to the data protection rights and freedoms of citizens of the EU, we agree to assist you in a reasonable and timely manner to conduct a data protection impact assessment, which may include consulting with the relevant data protection authority.

Your Obligations

As a Controller under the GDPR, you are required to carry out certain responsibilities and to comply with certain requirements. For example, and without intending to limit your obligations, you are required to comply with the privacy and confidentiality provisions of the GDPR, just as we are. You are also required to ensure that the consent of Data Subjects is obtained and that collection of Your Personal Data is otherwise justified under the GDPR. We acknowledge that in doing so, you are required to ensure that your Processors also comply with certain requirements, and we agree to reasonably cooperate with your requests in this regard. However, if you make requests of us that go beyond our obligations set forth in the “Our GDPR Obligations” section of this DPA, we will comply with your requests at your expense.

EXHIBIT A

Commission Decision C(2010)593 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. These clauses are incorporated into the data processing agreement agreed by the parties, and signatures hereto are presumed.

The customer of Eddy HR, as described in the Eddy HR Terms of Service (the “data exporter”)

And Eddy HR, LLC

Address:

Tel.: 877-750-3339; E-mail privacy@eddy.com

(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.

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 data¹;

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

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

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.

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

Clause 5

Obligations of the data importer²

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial

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, defence, 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.

information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses³. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore. Notwithstanding the foregoing, certain of Your Personal Information is subject to the laws of various jurisdictions regarding archiving of employment-related data. To comply with that broad array of laws, and to allow Company to facilitate the restarting of clients who may have terminated their agreement with Company, Company keeps the employment-related data for a period of seven years, unless a client makes a request to delete that data, in which case Company will delete the data within thirty (30) days after receipt of the request.

³ This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Signatures Presumed

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.

Data exporter

The data exporter is the customer, as defined in the Eddy HR Terms of Use (“Agreement”).

Data importer

The data importer is Eddy HR, Inc., a human resources management service in which the Service stores personal information, supporting documentation of the customer, time off, and employee reviews for the purposes of centralizing human resources data to the organization in accordance to the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter’s prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter’s Users authorized by data exporter to use the Services

Categories of data

The personal data transferred include, but not limited to, the following categories of data:

- First, Middle, and Last Name
- Title
- Position
- Employer
- Contact Information (Company, email, phone, physical home address)
- ID Data
- Professional Life data
- Personal Life data
- Connection data
- Localization data

Special categories of data (if appropriate)

The personal data transferred include, but not limited to, the following special categories of data:

- Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or

ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

Signatures Presumed

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The parties' signature is presumed.

The technical and organizational measures to be implemented by data importer are described in Exhibit B of the DPA entered into by the parties.

Signatures Presumed

EXHIBIT B

Security Measures

The security measures we take are outlined on our website at <https://eddyhr.com/security/>. Those measures are periodically updated to ensure we are following current standards in data security.

EXHIBIT C
List of SubProcessors

| Subprocessor | Services provided to Vendor | Location of the Processing (country) |
|---------------|---------------------------------------------------|--------------------------------------|
| Amazon | Data storage and infrastructure | USA |
| Stripe | PCC compliance and payment processing | USA |
| HelloSign | Data storage and processing | USA |
| Indeed | Data storage and processing | USA |
| Glassdoor | Data storage and processing | USA |
| Nuevoo | Data storage and processing | Canada |
| Hubspot | E-mail marketing, CRM, web forms to capture leads | USA |
| Airtable | Marketing services | USA |
| Outreach | Sales services | USA |
| ZenDesk, Inc. | Customer support | USA |