# POCKET RECRUITER

## DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") forms part of the Subscription Agreement ("SA") between the Subscriber and Pocket to reflect the parties' agreement regarding the Processing of Subscriber's Personal Data, in accordance with the requirements of Data Protection Laws in the Supported Jurisdictions.

Subscribers located in the European Union or the European Economic Area enter into this agreement which includes the Standard Contractual Clauses adopted by the European Commission as directed by Article 46, EU GDPR, "Transfers subject to appropriate safeguards" with respect to the data processed under this Subscription Agreement.

### THIS DPA INCLUDES:

(i) Standard Contractual Clauses, attached as EXHIBIT C-1.

(a) Appendix 1 to the Standard Contractual Clauses, which includes specifics on the personal data transferred by the data exporter to the data importer.

(b) Appendix 2 to the Standard Contractual Clauses, which includes a description of the technical and organizational security measures implemented by the data importer as referenced.

(ii) List of Subcontractors, attached as EXHIBIT C-2.

### Definitions

This DPA relies on the following definitions with respect to the terms governing the processing of Personal Data:

"**Data Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means the Pocket entity which Processes Personal Data on behalf of the Data Controller.

"**Data Protection Laws**" means all laws and regulations, including laws and regulations of the United States, European Union, the European Economic Area and their member states, applicable to the Processing of Personal Data under the Agreement.

"**Data Subject**" means the individual to whom Personal Data relates.

"**Personal Data**" means any information relating to an identified or identifiable person.

“**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (“Process”, “Processes” and “Processed” shall have the same meaning).

“**Sub-processor**” means any Data Processor engaged by Pocket.

## Scope and Responsibility

Processor shall process Personal Data on behalf of Controller. Processing shall include such actions as may be specified in the Subscription Agreement. Within the scope of the Subscription Agreement, Controller shall be solely responsible for complying with the statutory requirements relating to data protection, regarding the transfer of Personal Data to the Processor and the Processing of Personal Data (acting as “responsible body” as defined in § 3 para. 7 BDSG” or a corresponding provision of the otherwise applicable national data protection law).

Based on this responsibility, Controller shall be entitled to demand the rectification, deletion, blocking and making available of Personal Data during and after the term of the Subscription Agreement in accordance with the further specifications of such agreement on return and deletion of personal data.

The regulations of this DPA shall equally apply if testing or maintenance of automatic processes or of Processing equipment is performed on behalf of Controller, and access to Personal Data in such context cannot be excluded.

## Processors Responsibilities

Processor shall collect, process and use Personal Data only within the scope of Controller’s Instructions. If the Processor thinks that an instruction of the Controller infringes the BDSG or other data protection provisions, it shall point this out to the principal without delay.

Within Processor’s area of responsibility, Processor shall structure Processor’s internal corporate organization to ensure compliance with the specific requirements of the protection of Personal Data. Processor shall take the appropriate technical and organizational measures to adequately protect Controller’s Personal Data against misuse and loss in accordance with the requirements of the German Federal Data Protection Act (§ 9 BDSG) or a corresponding provision of the otherwise applicable national data protection law. Such measures hereunder shall include, but not be limited to,

a) the prevention of unauthorized persons from gaining access to Personal Data Processing systems (physical access control),

b) the prevention of Personal Data Processing systems from being used without authorization (logical access control),

c) ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control),

d) ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),

e) ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems (entry control),

f) ensuring that Personal Data Processed are Processed solely in accordance with the Instructions (control of instructions),

g) ensuring that Personal Data are protected against accidental destruction or loss (availability control),

h) ensuring that Personal Data collected for different purposes can be processed separately (separation control).

A measure as referred to in points b to d above shall be in particular, but shall not be limited to, the use of state of the art encryption technology for client access. An overview of the above listed technical and organizational measures is attached to this DPA in Exhibit C-1 Appendix 1.
Upon Controller's request, Processor shall provide a current Personal Data protection and security program covering Processing hereunder.

Upon Controller's request, and except where Controller can obtain such information directly, Processor shall provide all information necessary for compiling the overview defined by § 4g para. 2 sentence 1 BDSG or a corresponding provision of the otherwise applicable national data protection law.

Processor shall ensure that any personnel entrusted with Processing Controller's Personal Data have undertaken to comply with the principle of data secrecy in accordance with § 5 BDSG (or a corresponding provision of the otherwise applicable national data protection law) and have been duly instructed on the protective regulations of the BDSG or the otherwise applicable national data protection law. The undertaking to secrecy shall continue after the termination of the above-entitled activities.

The Processor shall appoint a data protection official, if this is legally required and, upon request of Controller, Processor shall notify to Controller the contact details of the data protection official.

Processor shall, without undue delay, inform Controller in case of a serious interruption of operations or violations by the Processor or persons employed by it of provisions to protect Personal Data or of terms specified in this DPA. In such an event, Processor shall implement the measures necessary to secure the Personal Data and to mitigate potential adverse effects on the data subjects and shall agree upon the same with Controller without undue delay. Processor shall support Controller in fulfilling Controller's disclosure obligations under section 42a BDSG (or a corresponding provision of the otherwise applicable national data protection law).

Controller shall retain title as to any carrier media provided to Processor as well as any copies or reproductions thereof. Processor shall store such media safely and protect them against unauthorized access by third parties. Processor shall, upon Controller's request, provide to Controller all information on Controller's Personal Data and information. Processor shall be obliged to securely delete any test and scrap material based on an Instruction issued by Controller on a case-by-case basis. Where Controller so decides, Processor shall hand over such material to Controller or store it on Controller's behalf.

Processor shall be obliged to audit and verify the fulfilment of the above-entitled obligations and shall maintain an adequate documentation of such verification.

## Controller's Responsibilities

Controller and Processor shall be separately responsible for conforming with such statutory data protection regulations as are applicable to them.
Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data detected during a verification of the results of such Processing.
Controller shall be obliged to maintain the publicly available register as defined in § 4g para. 2 sentence 2 BDSG (or a corresponding provision of the otherwise applicable national data protection law).
Controller shall be responsible for fulfilling the duties to inform resulting from § 42a BDSG or a corresponding provision of the otherwise applicable national data protection law.
Controller shall, upon termination or expiration of the SA and by way of issuing an Instruction, stipulate, within 30 days, the reasonable measures to return data carrier media or to delete stored data.
Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the SA shall be borne by Controller.

## Data Subject Rights

Where Controller, based upon applicable data protection law, is obliged to provide information to an individual about the collection, processing or use or its Personal Data, Processor shall assist Controller in making this information available, provided that: (i) Controller has instructed Processor in writing to do so, and (ii) Controller reimburses Processor for the costs arising from this assistance.

Where a data subject requests the Processor to correct, delete or block Personal Data, Processor shall refer such data subject to the Controller.

## Audit Responsibilities

Controller shall, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organizational measures taken by Processor, and shall document the resulting findings.

For such purpose, Controller may:

- obtain information from the Processor,
- request Processor to submit to Controller an existing attestation or certificate by an independent professional expert, or
- upon reasonable and timely advance agreement, during regular business hours and without interrupting Processor's business operations, conduct an on-site inspection of Processor's business operations or have the same conducted by a qualified third party which shall not be a competitor of Processor.

Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit.

## Subcontractors

Processor shall be entitled to subcontract Processor's obligations defined in the TOU Provided to third parties only with Controller's written consent.

Controller consents to Processor's subcontracting to Processor's affiliated companies and third parties, as listed in Exhibit C-2, of Processor's contractual obligations hereunder.

If the Processor intends to instruct subcontractors other than the companies listed in Exhibit C-2, the Processor must notify the Controller thereof in writing (email to the email address(es) on record in Processor's account information for Controller is sufficient) and must give the Controller the possibility to object against the instruction of the subcontractor within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the Controller proves that significant risks for the protection of its Personal Data exist at the subcontractor). If the Processor and Controller are unable to resolve such objection, either party may terminate the TOU by providing written notice to the other party. Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

Where Processor engages subcontractors, Processor shall be obliged to pass on Processor's contractual obligations hereunder to such subcontractors. Sentence 1 shall apply in particular, but shall not be limited to, the contractual requirements for confidentiality, data protection and data security stipulated between the parties of the TOU.

Where a subcontractor is used, the Controller must be granted the right to monitor and inspect the subcontractor in accordance with this DPA and Section 11 BDSG in conjunction with item No 6 of the Annex to Section 9 BDSG (or in accordance with the corresponding provision of the

otherwise applicable national data protection law). This also includes the right of the Controller to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations within the subcontract relationship, where necessary by inspecting the relevant contract documents.

The provisions of this § 7 shall apply as well if a subcontractor in a third country shall be instructed. The Controller hereby authorizes the Processor, to agree in the name and on behalf of the Controller with a subcontractor which processes or uses Personal Data of the Controller outside of the EEA, to enter into EU Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries dated 5 February 2010. This applies accordingly from the date of this authorization with respect to EU Standard Contractual Clauses (Processors) already concluded by the Processor with such subcontractors.

## Duties to Inform, Mandatory Written Form, Choice of Law, Additional Terms

Where Controller's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed, Processor shall inform Controller without undue delay. Processor shall, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in Controller's sole property and area of responsibility, that Personal Data is at Controller's sole disposition, and that Controller is the responsible body in the sense of the BDSG (or a corresponding provision of the otherwise applicable national data protection law).

In case of any conflict, the regulations of this DPA shall take precedence over the regulations of the TOU. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

The Standard Contractual Clauses in Exhibit C1 – Standard Contractual Clauses (Processors) ("**SCCs**") will apply to the processing of Personal Data by Processor under the TOU. Upon the incorporation of this DPA into the TOU, the parties indicated in § 9 below (Parties to this DPA) are agreeing to the SCCs and all appendixes attached thereto. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Exhibit C1, the SCCs shall prevail.

The SCCs apply only to Personal Data that is transferred from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive), and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to binding corporate rules for processors.

## Parties to this DPA

This DPA is an amendment to and forms part of the TOU. Upon the incorporation of this DPA into the TOU (i) Controller and Pocket's entity that are each a party to the TOU are also each a

party to this DPA, and (ii) Pocket is a party to this DPA, but only with respect to agreement to the SCCs pursuant to § 8 of the DPA, this section § 9 of the DPA, and to the SCCs themselves.

If Pocket is not a party to the TOU, the section of the TOU entitled 'Limitation of Liability' shall apply as between Controller and Pocket, and in such respect any references to 'Pocket', 'Pocket Recruiter', 'we', 'us' or 'our' shall include both Pocket Recruiter, Inc. and the Pocket entity that is a party to the TOU.

The legal entity agreeing to this DPA as Controller represents that it is authorized to agree to and enter into this DPA for; and is agreeing to this DPA solely on behalf of, the Controller.

# Exhibit C1 - 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,

**The Subscriber, as defined in this Subscription Agreement (the "Data Exporter")**

And

**Pocket, as defined in this Subscription Agreement. (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 data;

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

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

(d) 'the 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 organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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

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.
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.
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.
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 organizational 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, unauthorized 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 importer**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

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

(c) that it has implemented the technical and organizational 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 unauthorized access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

## Clause 6

### Liability

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

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.
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.
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**

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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.

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.

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**

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.

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.

# Exhibit C1 - Appendix 1 to Standard Contractual Clauses

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

**A. Data exporter**

The data exporter is the Subscriber, as defined in the Service Agreement.

**B. Data importer**

The data importer is Pocket as described in the Service Agreement.

**C. Data subjects**

The personal data transferred concern the Data Exporter's end users including employees, contractors and the personnel of customers, suppliers, collaborators, and subcontractors. Data Subjects also includes Data Exporter's clients, potential job candidates, job applicants, and individuals attempting to communicate with or transfer personal information to the Data Exporter's end users.

**D. Categories of data**

The personal data transferred concern personal data, entity data, navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Site.

**E. Special categories of data (if appropriate)**

The parties do not anticipate the transfer of special categories of data.

**F. Processing operations**

With respect to personal data of non-German end users as data exporters, the following provisions apply:

> The personal data transferred will be subject to the following basic processing activities:
>
> **Scope of Processing**
>
> Personal data may be processed for the following purposes: (a) to provide the Site (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under Pocket's TOU.
>
> The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or its sub processors maintain facilities as necessary for it to provide the Site.
>
> **Term of Data Processing**

Data processing will be for the term specified in Pocket's Terms of Use under Exhibit A ("**TOU**"). For the term of Pocket's TOU, and for 30 days after the expiry or termination of Pocket's TOU, the Data Importer will provide the Data Exporter the option to request an export of the Data Exporter's personal data processed pursuant to Pocket's TOU.

**Data Deletion**

For the term of Pocket's TOU, the Data Importer will provide the Data Exporter with the ability to delete data as detailed in Pocket's TOU.

**Access to Data**

For the term of Pocket's TOU, the Data Importer will provide the Data Exporter with the ability to correct, block, export and delete the Data Exporter's personal data from the Site in accordance with Pocket's TOU.

**Sub processors**

The Data Importer may engage sub processors to provide parts of the Site. The Data Importer will ensure sub processors only access and use the Data Exporter's personal data to provide the Data Importer's products and services and not for any other purpose.

With respect to personal data of German end users as data exporters, the following provisions apply:

**Specification of processing activities in accordance with Section 11 BDSG**

Taking into account the requirements of Section 11 German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) on commissioned data processing, the processing activities are specified as follows:

**Subject and duration of the commission**
Personal data may be processed for the following purposes: (a) to provide the Site (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under Pocket's TOU.

The Clauses have been concluded for the duration of the respective service agreement (Pocket Customer Terms of Service).

**Extent, type and purpose of the planned collection, processing or use of data; the type of data and group of persons affected**
See for the type of data and group of persons affected the descriptions included in this Appendix 1 under the headings "Categories of data" and "Data subjects".

The purpose of the processing is: (a) to provide the Site (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under Pocket's TOU.

**Technical and organizational measures to be taken under Section 9 BDSG**
The Data Importer will take the appropriate technical and organizational measures to adequately protect data exporter's Personal Data against misuse and loss in accordance with the requirements of Section 9 BDSG. See Exhibit C1 - Appendix 2 for details.

**Correction, erasure and blocking of data**
Where a data subject requests the Data Importer to correct, delete or block data, the Data Importer shall refer such data subject to the data exporter. Deletion, blocking and correction of personal data by the Data Importer shall only happen upon instruction of the data exporter.

**Agent's obligation under sub-Section 4 (of Section 11 BDSG), in particular controls to be undertaken**
See Appendix 2 for details.

The Data Importer has obliged its employees employed in data processing not to collect, process or use personal data without authorization (data confidentiality). This obligation continues to be valid after termination of the respective employment relationship.

**Right to issue subcontracts**
See Clauses 5 (h) and 11 of the Clauses. The data exporter already agrees to subcontracting the data processors listed in Exhibit C2.

If the Data Importer intends to instruct subcontractors other than the companies listed in Exhibit C2, the Data Importer must notify the data exporter thereof in writing (email to the email address(es) on record in the Data Importer's account information for data exporter is sufficient) and must give the data exporter the possibility to object against the instruction of the subcontractor within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the data exporter proves that significant risks for the protection of its personal data exist at the subcontractor). If the Data Importer and data exporter are unable to resolve such objection, either party may terminate the TOU by providing written notice to the other party. data exporter shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

**Principal's rights of control and the agent's corresponding obligations to tolerate and cooperate**
See Clauses 5 (e) and (f) of the Clauses.

**Violations by the agent or persons employed by him/her of provisions to protect personal data or of terms specified in the commission which must be reported**
See Clause 5 (d) of the Clauses.

**Extent of the principal's authority to issue instructions to the agent**
Personal data can only be processed by the Data Importer based upon instructions of the data exporter. Except as legally required, personal data may be processed or used for another purpose, including disclosure to third parties, only with the prior written approval of the data exporter. Copies of the personal data shall not be made without consent of the data exporter, except for copies which are necessary for the processing or if required to comply with statutory retention obligations.

**Return of data storage media and the erasure of data stored by the agent after the commission has been completed.**
Data exporter shall be entitled to demand the rectification, deletion, blocking and making available of personal data during and after the term of the respective service agreement (Pocket Customer Terms of Service) in accordance with the further specifications of such agreement on return and deletion of personal data.

# Exhibit C1 - Appendix 2 to Standard Contractual Clauses

This Appendix forms part of the Clauses.

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

Pocket currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by Data Exporter, Pocket may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices.

**a) Access Control**

i) **Preventing Unauthorized Product Access**

Outsourced processing: Pocket hosts its Service on the Amazon Web Services Cloud (AWS). The service is deployed into separate AWS Regions which process and hold Customer Data according for their region. For instance, Subscriber's processing data in the European Union or the European Economic Area are hosted in EU based AWS Regions such as EU (Ireland) and EU (London). Subscriber's processing United States data are hosted in U.S. based AWS Regions such as US East (N. Virginia).

Physical and environmental security: Pocket secures all access to hosts within AWS using a Virtual Private Network (VPN) which requires individually issued certificates.

Authentication: Pocket has implemented a uniform password policy for all access to its products. Customers who interact with the products via the user interface must authenticate before accessing any data including non-public customer data.

Authorization: Customer data is only accessible to Customers via the application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. All User and Customer data is tagged at creation with a unique customer ID which is validated for access against a User's credentials. All application features are also privilege driven and can only be accessed by authorized Users with access rights. Every access and

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) **Preventing Unauthorized Product Use**

Pocket implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between data center providers and include Virtual Private Cloud (VPC) implementations and security group assignment, along with traditional enterprise firewall and Virtual Local Area Network (VLAN) assignment.

Intrusion detection and prevention: Pocket implemented a Web Application Firewall (WAF) solution to protect all hosted sites as well as Pocket Service access. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in Pocket's source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: Pocket maintains relationships with industry recognized penetration testing service providers for semi-annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) **Limitations of Privilege & Authorization Requirements**

Product access: A subset of Pocket's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, and to detect and respond to security incidents. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

Personnel: All Pocket employees and contractors are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards. All employees and contractors attend Security and Data Privacy training at least once per year as well as when regulations change.

**b) Transmission Control**

In-transit: Pocket uses HTTPS encryption (also referred to as SSL or TLS) on all access to its applications and API implementations. Pocket's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Pocket encrypts stored user passwords and conforms to policies that follow at least industry standard practices for security.

**c) Input Control**

Detection: Pocket has designed its applications to generate extensive audit information about access and modification of all information stored by its services. Additionally, Pocket logs and tracks information about system access, system behavior, traffic received, system authentication, and all other application requests. Monitoring systems review log data and alert appropriate employees of malicious, unintended, or anomalous activities. Pocket personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Pocket maintains a record of all known security incidents that includes description, dates and times, records of relevant activities, and related data. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Pocket will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Pocket becomes aware of unlawful access to Customer data stored within its products, Pocket will: 1) notify the affected Customers of the incident; 2) provide a description of the steps Pocket is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Pocket deems necessary. Notification(s) of incidents, if any, will be delivered to one or

more of the Customer's contacts in a form agreed with Customers, which may include emails and phone calls.

**d) Personal Data Control**

Pocket deems all Customer data as owned by the Customer and never sells or provides personal data to any third party. Any Customer data is only provided to the owner's request after validating the authenticity of each request.

Terminating Customers: Core Customer Data in active (i.e., primary) databases is purged upon a customer's written request, or 30 days after a customer terminates all agreements with Pocket. Information stored in backups, replicas, and snapshots is not automatically purged, but instead ages out of the system as part of the data lifecycle. Pocket reserves the right to alter data purging period in order to address technical, compliance, or statutory requirements.

**e) Availability Control**

Infrastructure availability: AWS will use commercially reasonable efforts to make the Included Products and Services each available with a Monthly Uptime Percentage of at least 99.99%. Pocket uses multiple availability zones for each Region to insure its infrastructure is available at least as much as AWS.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones within the Customer's Region.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Pocket's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Pocket operations in maintaining and updating the product applications and backend while limiting downtime.

**f) Separation in Processing**

Pocket's analysis of Customer Data is used to provide and improve its services and does not collect Personal Data but rather generates aggregate data that is none specific to any one customer or individual. Pocket does not use that data for other purposes that would require separate processing.

## Exhibit C2 – List of Subcontractors

- Amazon Web Services, Inc.