Data Processing Addendum ("Addendum")

Between _____ ("**Company**")

and

Pipedrive OÜ ("**Pipedrive**")

(Company and Pipedrive also referred to as a "**Party**" and collectively as the "**Parties**"

1. Background

The Parties have agreed to the Terms of Service posted at https://www.pipedrive.com/en/terms-of-service ("**Framework Agreement**") according to which Pipedrive has agreed to provide certain services to Company (hereinafter the "**Services**").

When providing the Services, Pipedrive may collect, process and gain access to personal data of individuals on behalf of Company. From a data protection perspective, Company will be the data controller and Pipedrive will be the data processor.

This Data Processing Addendum specifies the data protection obligations of the Parties under the Framework Agreement. It applies to all activities performed by Pipedrive in connection with the Framework Agreement in which Pipedrive, its staff or a third party acting on behalf of Pipedrive comes into contact with personal data of individuals.

If there is a conflict between the terms of the Framework Agreement and those of this Data Processing Addendum, the provisions of this Addendum will prevail.

2. Pipedrive's Obligations

2.1 Pipedrive will collect and process personal data in connection with the Framework Agreement only for the purpose of fulfilling the Framework Agreement. Pipedrive will carry out the data processing operations in accordance with the Framework Agreement as well as any written instructions received from Company that do not conflict with the provisions of this Data Processing Addendum or the Framework Agreement.

2.2 Personal data to which Pipedrive may receive access concern the following data subjects ("**Data Subjects**"):

- 2.2.1 Company's directors, officers, employees, interns, trainees, agents, contractors, job applicants, customers, suppliers, subcontractors, business contacts;
- 2.2.2 Company's customers' directors, officers, employees, interns, trainees, agents, contractors, customers or business contracts;
- 2.2.3 Any third party with whom Pipedrive interacts or is requested to interact in connection with the provision, operation, or maintenance of the Services on behalf of Company;
- 2.2.4 Any other individuals for which Company enters personal data or information into the Service.

Pipedrive will not have any knowledge or control over the categories or identities of the Data Subjects whose Personal Data Company may elect to record or upload into the Service, except as provided in the Framework Agreement.

2.3 The data processing activities will generally include the following categories of personal data ("**Personal Data**"):

- 2.3.1 Name, street address, email address, phone number, other contact information, company name, title;
- 2.3.2 Customer history;
- 2.3.3 Contract billing and bank data;

2.3.4 IP Addresses;
2.3.5 References, meeting notes; and
2.3.6 Such categories of personal data pertaining to an identified or identifiable individual as Company or Company's representative may enter or upload from time to time into the Service.

Pipedrive will not have any knowledge or control over the categories or nature of the Personal Data that Company may elect to record or upload into the Service, except as provided in the Framework Agreement.

2.4 Pipedrive will not collect, process or use any Personal Data made available to it for any purposes other than for the performance of the Services. Copies or duplicates of any Personal Data made available hereunder may only be compiled with the approval of Company or as permitted under the Framework Agreement.

2.5 Pipedrive will grant to Company and its designees during the term of the Data Processing Addendum all requested information and access rights strictly in accordance with Pipedrive's security policy in order to verify Pipedrive's compliance with the Framework Agreement, this Data Processing Addendum and with applicable data protection law. Company may determine Pipedrive's compliance with the agreed technical and organizational measures (see **Exhibit 1** of this Data Processing Addendum) at Pipedrive's facilities. If and to the extent Company engages third parties to conduct the audit, such third parties have to be bound to confidentiality obligations similar to those agreed for Pipedrive under this Data Processing Addendum.

2.6 Pipedrive will notify Company without undue delay if Pipedrive is of the opinion that a written instruction received from Company is in violation of applicable data protection law and/or in violation of contractual duties under the Framework Agreement.

2.7 Pipedrive will notify Company without undue delay if Pipedrive becomes aware that Pipedrive's employees have violated any data protection law, or the provisions of the Framework Agreement if the violation occurs in the course of the processing of the data by Pipedrive. Furthermore, if Pipedrive is of the opinion that Personal Data have been or might have been illegally transferred or otherwise illegally disclosed to or accessed by a third party, Pipedrive will notify Company thereof without undue delay in accordance with applicable data protection laws, including Regulation (EU) 2016/679. In case of any loss of, or unauthorized access to Personal Data stored on the Service, Pipedrive will inform Company without undue delay, and assist Company in fulfilling its statutory obligations under applicable data protection laws, including Regulation (EU) 2016/679.

2.8 Company grants Pipedrive a general authorization in line with Article 28 (2) of Regulation (EU) 2016/679 to engage processors for the purposes of providing the Pipedrive Services. Pipedrive will inform Company of changes in such processors in the Framework Agreement in accordance with the procedure of modifying the Framework Agreement.

2.9 Pipedrive may only engage Subcontractors for providing the Services under the Framework Agreement if Pipedrive (i) communicates the name, address and contact details of the subcontractor and the tasks of the subcontractor prior to engaging the subcontractor, (ii) has in place or concludes prior to engaging the subcontractor a sub--processing agreement between Pipedrive and the subcontractor that is no less protective with respect to Company's interest and protection of Personal Data than this Data Processing Addendum, (iii) ensures that an adequate level of data protection for subcontractors that are located outside of the EU/EEA exists or is created (e.g. by concluding EU Standard Contractual Clauses or by selecting subcontractors that are certified under the Privacy Shield framework) (iv) has sufficient rights against the subcontractor to enforce a claim or request of Company in the context of the Services provided by the subcontractor and (v) provides copies of documentation evidencing (ii) to (iv) above before engaging the subcontractor.

2.10 Pipedrive will keep confidential and will not make available any Personal Data received in connection with the Framework Agreement to any third party except as required by applicable law.

2.11 Pipedrive will support Company in fulfilling the rights of the Data Subject, in particular with regard to correction, blocking, deletion, and provision of Personal Data. If so instructed by Company, and

if feasible, Pipedrive will correct, block or delete Personal Data in accordance with Company's written instructions. If a Data Subject contacts Pipedrive directly in order to have his or her data corrected, deleted or blocked, Pipedrive will forward such request to Company without undue delay after receipt of such request. Pipedrive will assist Company in ensuring compliance with the obligations pursuant to Articles 32-36 of Regulation (EU) 2016/679 taking into account the nature of processing and the information available to Pipedrive.

2.12 Pipedrive will adopt adequate technical and organizational measures to ensure the security of its network and data centre operations for the purposes of providing the Services to Company in accordance with **Exhibit 1**.

2.13 Pipedrive will use reasonable efforts to fully cooperate and to comply with any instructions, guidelines and orders received from the relevant supervisory authority when such instructions, guidelines or orders pertain to the Personal Data.

2.14 Upon termination of the Framework Agreement or, if applicable, an agreed exit phase, upon written instruction from Company, Pipedrive will return all media provided by Company with regard to the Framework Agreement containing Personal Data and will destroy any other Personal Data within 6 months of termination of the Framework Agreement.

2.15 Pipedrive will use qualified personnel with data protection training to provide the Services.

2.16 Pipedrive will oblige its employees to process and use the Personal Data only in accordance with the Framework Agreement, this Data Processing Agreement, including its exhibits, and any written instructions received from Company.

3. Obligations of Company

3.1 Company will be responsible for the evaluation of the admissibility of the data processing and for ensuring the rights of the data subjects concerned.

3.2 Company will be entitled to issue written instructions regarding the scope and the procedure of the data processing.

4. Technical and Organizational Measures

Pipedrive will implement the technical and organizational security measures as set forth in **Exhibit 1** to this Data Processing Addendum. The technical and organizational security measures will be aimed at protecting the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing. Upon Company's request, but not more frequently than once in any twelve (12) month period, Pipedrive will provide a self-audit report or a third--party report confirming compliance with the technical and organizational security measures before processing or accessing any Personal Data on behalf of Company.

5. Term

This Data Processing Addendum will become effective when signed by the Parties ("**Effective Date**") and will run for the same term as the Framework Agreement.

6. Choice of Law

The Data Processing Addendum is governed by the law indicated as the governing law in the respective provisions of the Framework Agreement.

[signature page to follow]

	Pipedrive OÜ
Company	Pipedrive
	Martin Ojala
Name	Name
	Data Protection Officer
Position	Position
	28 August 2019
Date	Date
	
Signature	Signature

EXHIBIT 1 to Data Processing Addendum

Technical and Organizational Measures

Description of the technical and organizational security measures implemented by

Pipedrive according to Sec. 4 of the Data Processing Addendum:

1. Access Control of Processing Areas

Pipedrive will implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the Personal Data are processed or used. This will be accomplished by:

- establishing security areas;
- protection and restriction of access paths;
- securing the decentralized telephones, data processing equipment and personal computers;
- establishing access authorizations for employees and third parties, including the respective documentation;
- regulations on card--keys;
- restriction on card--keys;
- all access to the data centre where personal data are hosted is logged, monitored, and tracked;
- the data centre where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

2. Access Control to Data Processing Systems

Pipedrive will implement suitable measures to prevent its data processing systems from being used by unauthorized persons. This will be accomplished by:

- identification of the terminal user to the data importers systems;
- automatic time--out of user terminal if left idle, identification and password required to reopen;
- automatic turn--off of the user ID when several erroneous passwords are entered, log file of events, (monitoring of break--in--attempts);

3. Access Control to Use Specific Areas of Data Processing Systems

Pipedrive will ensure that the persons entitled to use the Pipedrive data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization). Pipedrive will ensure that Personal Data cannot be read, copied or modified or removed without authorization. This will be accomplished by:

- employee policies and training in respect of each employee’s access rights to the personal data;
- effective and measured disciplinary action against individuals who access personal data without authorization;

- release of data to only authorized persons;
- control of files, controlled and documented destruction of data; and
- policies controlling the retention of back--up copies.

4. Transmission Control

Pipedrive will implement suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This will be accomplished by:

- use of state--of--the--art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- monitoring of the completeness and correctness of the transfer of data (end-to-end check).

5. Input Control

Pipedrive will implement suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed. This will be accomplished by:

- an authorization policy for the input of data into memory, as well as for the reading, alteration and deletion of stored data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of user codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log--off of user ID's that have not been used for a substantial period of time; and
- proof established within data importers' organization of the input authorization;

6. Job Control

Pipedrive will implement suitable measures to ensure that the Personal Data are processed strictly in accordance with the instructions of Company. This will be accomplished by:

- ensuring clear instructions to Pipedrive regarding the scope of any processing of Personal Data. This will be limited to specific system development and database management requirements of Company (for example, the creation of new reporting templates, where processing of data in necessary in order to test those reporting templates); and
- granting regular access and control rights to Company, on appropriate notice and in accordance with Company's security policies and accompanied by Pipedrive.

7. Availability Control

Pipedrive will implement suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This will be accomplished by:

- infrastructure redundancy: two clustered database servers will be used for storing the data;
- tape backup is stored off--site and available for restore in case of failure of database server.

8. Separation of Processing for different Purposes

Pipedrive will implement suitable measures to ensure that data collected for different purposes can be processed separately. This will be accomplished by:

- access to data will be separated through application security for the appropriate users;
- modules within Pipedrive's database will separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data will be stored in different normalized tables, separated per module or function they support; and
- interfaces, batch processes and reports will be designed for only specific purposes and functions, so data collected for specific purposes is processed separately.