DATA PROCESSING AGREEMENT (DPA)

CONSIDERATIONS

This Data Processing Agreement (hereafter: "**DPA**") is an annex to the Teamleader Focus Terms of Service (available here). Together, the Terms of Service and the DPA constitute the Agreement with the Customer.

Within the context of the performance of the Services for the Customer, TEAMLEADER shall have access to Personal Data and/or will have to Process these Personal Data, for which the Customer is responsible as 'Controller' in accordance with (i) the General Data Protection Regulation of 27 April 2016 ('the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the Processing of personal data and on the free movement of such data or 'GDPR') and (ii) all Belgian laws regarding the implementation of the GDPR (hereafter jointly referred to as the "**Privacy Legislation**").

Through this DPA Parties wish to determine in writing their mutual agreements with regard to (i) managing, securing and/or Processing of such Personal Data and (ii) Parties' obligation to comply with the Privacy Legislation.

Note that this DPA deals only with TEAMLEADER's role as Processor and not as a Controller. For more information about TEAMLEADER's Processing of Personal Data in its capacity as a Controller, please refer to the Privacy Statement.

THEREFORE, PARTIES HAVE AGREED AS FOLLOWS

1 DEFINITIONS

In this DPA, the following concepts have the meaning described in this article (when written with a capital letter):

'**Agreement**', '**Customer**', '**Customer Account**', '**Customer Account Data**', '**Lead Capture Booster**', '**Party**' / '**Parties**', '**Services**', '**Subscription**', '**TEAMLEADER**', **'Term'** and '**Tool**' shall have the meaning given to them in the Terms of Service.

For the purpose of this DPA only, '**Personal Customer Account Data**' shall mean all Personal Data for which the Customer is responsible as 'Controller' and which Teamleader expects to Process on behalf of the Customer in the context of providing its Services, a non-limitative list of which can be found in Overview I. For the avoidance of any doubt, this definition is broader than the one used in the Terms of Service, because it also includes certain Personal Data of Users.

'**Controller**', '**Data Subject**', '**Data Breach**', '**Personal Data**', '**Processor**' and '**Process/Processing**' shall have the meaning given to them in the Privacy Legislation.

Integration: A software integration between the Tool and a third-party application that is enabled through the Tool's application programming interface ("API").

Marketplace: The Teamleader Focus marketplace available via marketplace.teamleader.eu where the Customer can select from the range of different Optional Integrations.

Optional Integration: An Integration which the Customer selects and enables on its own initiative and which it can disable during the Term.

Standard Integration: An Integration which is automatically enabled when using the Services and which the Customer cannot disable during the Term.

Sub-Processor: Any Processor engaged by TEAMLEADER and authorized under this DPA to have logical access to and Process certain Personal Customer Account Data in order to provide parts of the Services and technical support. This includes, but is not necessarily limited to all Standard Integrations which Process Personal Customer Account Data.

This DPA includes the following overviews:

- **Overview I:**
  Overview of (i) the Personal Data which Parties expect to be subject of the Processing, (ii) the categories of Data Subjects which Parties expect to be subject of the Processing, (iii) the use (i.e. the way(s) of Processing) of the Personal Data, (iv) the goals and means of such Processing and (v) the term(s) during which the (different types of) Personal Data shall be stored;
- **Overview II:**
  Overview and description of the security measures taken by TEAMLEADER under this DPA.

2 ROLES OF THE PARTIES

Parties acknowledge and agree that with regard to the Processing of Personal Customer Account Data, the Customer shall be considered 'Controller' and TEAMLEADER 'Processor'. Further, TEAMLEADER is allowed to engage Sub-Processor(s) pursuant to the requirements set forth in **Article 6**.

3 USE OF THE SERVICES

3.1 The Customer acknowledges explicitly that:

- ✓ TEAMLEADER purely acts as a facilitator of its Services. Hence, the Customer shall be solely responsible for the use it makes of the Services;
- ✓ It shall be solely responsible to comply with all laws and regulations (such as but not limited to the retention period) imposed on it when using the Services.

3.2 In case of misuse by the Customer of the Services, the Customer agrees that TEAMLEADER can never be held liable in this respect nor for any damage that would occur from such misuse.

3.3 The Customer therefore undertakes to safeguard TEAMLEADER when such misuse would occur as well as for any claim from a Data Subject and/or third party due to such misuse.

4 OBJECT

4.1 The Customer acknowledges that as a consequence of using the Services, TEAMLEADER shall Process Personal Customer Account Data.

4.2 TEAMLEADER shall Process the Personal Customer Account Data in a proper and careful way and in accordance with the Privacy Legislation and other applicable rules concerning the Processing of Personal Data.

More specifically, TEAMLEADER shall – during the performance of the Services under the Agreement – provide all its know-how in order to perform the Services according to the rules of art, as it fits a specialized and 'good' Processor.

4.3 Nonetheless, TEAMLEADER shall only Process the Personal Customer Account Data upon request of the Customer and in accordance with its instructions, as described in **Overview I**, unless any legislation states otherwise.

4.4 The Customer, as Controller, owns and retains full control concerning (i) the Processing of Personal Customer Account Data, (ii), the types of Personal Customer Account Data Processed, (iii), the purpose of Processing and (iv) the fact whether such Processing is proportionate (non-limitative).

Moreover, the Customer shall be solely responsible to comply with all (legal) obligations in its capacity as Controller (such as but not limited to the retention period) and shall have the sole responsibility for the accuracy, quality, and legality of the Personal Customer Account Data, entered into the Tool, and the means by which it acquired such Personal Customer Account Data. The responsibility and control concerning the Personal Customer Account Data, subject to this DPA, shall thus never be vested in TEAMLEADER.

5 SECURITY OF PROCESSING

Taking into account the state of the art, TEAMLEADER implements appropriate technical and organizational measures for the protection of (i) Personal Customer Account Data – including protection against careless, improper, unauthorized or unlawful use and/or Processing and against accidental loss, destruction or damage – (ii) the confidentiality and integrity of Personal Customer Account Data, as set forth in **Overview II**.

6 SUB-PROCESSORS

6.1 The Customer acknowledges and agrees that TEAMLEADER may engage Sub-Processors in connection with the Agreement. In such a case, TEAMLEADER shall ensure that the Sub-Processors are at least bound by the same obligations by which TEAMLEADER is bound under this DPA.

6.2 TEAMLEADER undertakes to make a list of all Sub-Processors available in the Customer Account. Such a list shall include the identities of those Sub-Processors and their country of location. This list will always include all Standard Integrations which Process Personal Customer Account Data.

The Parties agree that the providers of Optional Integrations are not Sub-Processors within the meaning of this DPA. If Customer uses Optional Integrations to customize the Customer Account, a separate commercial relationship is established between the Customer and the provider of the Optional Integration. TEAMLEADER does not control if and how the Customer uses these Optional Integrations, and thus TEAMLEADER has no ownership to risk in this regard. The Controller is solely responsible for these Optional Integrations. TEAMLEADER recommends that Customer enters into a separate data Processing agreement with the providers of the Optional Integrations it selects.

6.3 TEAMLEADER undertakes to inform the Customer in writing of any intended change to the aforementioned list (e.g. adding or replacing a Sub-Processor).

The Customer is entitled to oppose a new Sub-Processor. As an exception to this rule, the Customer accepts that TEAMLEADER may engage other EU/EEA located companies in the Visma Group as Sub-Processors without prior approval or notification to the Customer.

If the Customer wishes to exercise its right to object, the Customer shall notify TEAMLEADER in writing and in a reasoned manner by the latest within ten (10) days upon receipt of TEAMLEADER's notice (cfr. **Article 6.3**).

6.4 In the event the Customer objects to a new Sub-Processor and such objection is not found unreasonable, TEAMLEADER, in consultation with the Customer, will make all reasonable efforts to resolve the Customer's objection.

If TEAMLEADER is, however, unable to resolve the Customer's objection, the Customer may terminate the Agreement on the condition that:

- ✓ The Services cannot be used by the Customer without appealing to the objected new Sub-Processor; and/or
- ✓ Such termination solely concerns the Services which cannot be provided by TEAMLEADER without appealing to the objected new Sub-Processor;

And this by providing written notice thereof to TEAMLEADER within a reasonable time.

7 DATA PROTECTION OFFICER

7.1 TEAMLEADER has appointed a data protection officer.

7.2 The appointed data protection officer may be reached at dpo@teamleader.eu.

8 TRANSFER OF PERSONAL CUSTOMER ACCOUNT DATA OUTSIDE THE EEA

Any transfer of Personal Customer Account Data outside the EEA to a recipient which residence or registered office does not fall under an adequacy decision issued by the European Commission, shall be governed by the terms of a data transfer agreement, which shall contain (i) standard contractual clauses pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 or (ii) other mechanisms foreseen by the Privacy Legislation and/or and other applicable rules concerning the Processing of Personal Data.

9 CONFIDENTIALITY

9.1 TEAMLEADER shall maintain the Personal Customer Account Data confidential and thus not disclose nor transfer any Personal Customer Account Data to third parties, without the prior written agreement of the Customer, unless:

- ✓ In case of an explicit written deviation from this confidentiality obligation (e.g. in the Terms of Service);
- ✓ Such disclosure and/or announcement is required by law or by a court or other government decision (of any kind). In such case TEAMLEADER shall, prior to any disclosure and/or announcement, discuss the scope and manner thereof with the Customer.

9.2 TEAMLEADER shall ensure that its personnel, engaged in the performance of the Services under the Agreement, are informed of the confidential nature of the Personal Customer Account Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. TEAMLEADER shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

9.3 TEAMLEADER shall ensure that its access to Personal Customer Account Data is limited to such personnel performing the Services under the Agreement in accordance with the DPA.

10 NOTIFICATION

10.1 TEAMLEADER shall use its best efforts to inform the Customer within a reasonable term when it:

- ✓ Receives a request for information, a subpoena or a request for inspection or audit from a competent public authority in relation to the Processing of Personal Customer Account Data;
- ✓ Has the intention to disclose Personal Customer Account Data to a competent public authority;
- ✓ Determines or reasonably suspects a Data Breach has occurred in relation to the Personal Customer Account Data.

10.2 In case of a Data Breach, TEAMLEADER:

- ✓ Notifies the Customer without undue delay after becoming aware of a Data Breach and shall provide – to the extent possible – assistance to the Customer with respect to its reporting obligation under the Privacy Legislation;
- ✓ Undertakes – as soon as reasonably possible – to take appropriate remedial actions to make an end to the Data Breach and to prevent and/or limit any future Data Breach.

11 RIGHTS OF DATA SUBJECTS

11.1 To the extent the Customer – in its use of the Services – does not have the ability to correct, amend, block or delete Personal Customer Account Data, as required by Privacy Legislation, TEAMLEADER shall – to the extent it is legally permitted to do so – comply with any commercially reasonable request by the Customer to facilitate such actions.

To the extent legally permitted, the Customer shall be responsible for any costs arising from TEAMLEADER's provision of such assistance.

11.2 TEAMLEADER shall, to the extent legally permitted, promptly notify the Customer if it receives a request from a Data Subject for access to, correction, amendment or deletion of that Data Subject's Personal Data. TEAMLEADER shall, however, not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to the Customer to which the Customer hereby agrees.

TEAMLEADER shall provide the Customer with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent the Customer does not have access to such Personal Data through its use of the Services.

To the extent legally permitted, the Customer shall be responsible for any costs arising from TEAMLEADER's provision of such assistance.

12 RETURN AND DELETION OF CUSTOMER ACCOUNT DATA

12.1 TEAMLEADER provides the Customer as much as possible with the option to delete Personal Data from the Customer Account during the lifetime of the Agreement. This allows the Customer to meet its own responsibilities regarding data minimization and storage limitation as a Controller.

12.2 Upon termination of the Subscription, the Customer has the possibility to export the Personal Customer Account Data (as well as other data, both personal and non-personal) from the Customer Account through the available export tools. This should be done before the Subscription ends.

12.3 Once the Subscription ends, TEAMLEADER shall first soft delete the Personal Customer Account Data during a period of thirty (30) calendar days. Restoring the Customer Account or providing an export of the Customer Account Data during this period of time can only be done with the assistance of TEAMLEADER, whereby TEAMLEADER can charge costs for the efforts made.

TEAMLEADER shall subsequently hard delete the Personal Customer Account Data at the earliest thirty (30) days and at the latest three (3) months after the Subscription has ended. Once the Personal Customer Account Data has been hard deleted, restoring the Customer Account or providing an export of the Customer Account Data is no longer possible.

13 CONTROL

13.1 TEAMLEADER undertakes to provide the Customer with all information required by the Customer to allow verification whether TEAMLEADER complies with the provisions of this DPA.

13.2 In this respect TEAMLEADER shall allow the Customer (or a third party on which the Customer appeals) to undertake inspections – such as but not limited to an audit – and to provide the necessary assistance thereto to the Customer or that third party.

To the extent legally permitted, the Customer shall be responsible for any costs arising from TEAMLEADER's provision of such assistance.

In any case, inspections must be conducted during regular business hours at the applicable facility, subject to TEAMLEADER's policies, and may not unreasonably interfere with TEAMLEADER's business activities.

14 MISCELLANEOUS

14.1 The DPA lasts as long as the Agreement has not come to an end. The provisions of this DPA shall apply to the extent necessary for the completion of this DPA and to the extent intended to survive the end of this DPA (such as but not limited to **Article 9** and **15**).

14.2 If one or more provisions of this DPA are found to be invalid, illegal or unenforceable, in whole or in part, the remainder of that provision and of this DPA shall remain in full force and effect as if such invalid, illegal or unenforceable provision had never been contained herein. Moreover, in such an event, Parties shall negotiate to replace the invalid provision by an equivalent provision in accordance with the spirit of this DPA. If Parties do not reach an agreement, then the competent court may mitigate the invalid provision to what is (legally) permitted.

14.3 Deviations, alterations and/or additions to this DPA shall only be valid and binding to the extent that they have been accepted in writing by both Parties.

14.4 This DPA and the corresponding rights and obligations that exist in respect of the Parties, cannot be transferred, directly or indirectly, without the prior written consent of the other Party.

14.5 (Repeatedly) non-enforcement by a Party or by both Parties of any right or provision of this DPA, can only be regarded as a toleration of a certain state, and does not lead to forfeiture

14.6 This DPA takes precedence over any other DPA between the Parties as well as over any conflicting provisions regarding the Processing of Personal Customer Account Data in other agreements or written communication between the Parties.

15 APPLICABLE LAW AND JURISDICTION

15.1 All issues, questions and disputes concerning the validity, interpretation, enforcement, performance or termination of this DPA shall be governed by and construed in accordance with Belgian law, without giving effect to any other choice of law or conflict-of-laws rules or provisions (Belgian, foreign or international) that would cause the laws of any country other than Belgium to be applicable.

15.2 Any dispute concerning the validity, interpretation, enforcement, performance or termination of this DPA shall be submitted to the exclusive jurisdiction of the courts of TEAMLEADER's registered office.

******

Overview I – Processing of Personal Customer Account Data by TEAMLEADER[1]

*This document entails an overview of the Personal Data TEAMLEADER is expected to Process **on behalf of** the Customer in the context of the Agreement as well as the categories of Data Subjects involved, the way(s) of Processing) of Personal Data, the means and purposes of Processing and the term during which the Personal Data shall be stored.*

I. Personal Data Processed

- **Personal Data of Users:**
  - Signature
  - Profile picture
  - Other Personal Data, depending on the use of the Services by the Customer (e.g. uploading or providing documents which contain Personal Data; entering descriptions of free fields such as in tasks, projects and time tracking which contain Personal Data; etc.)

- **Personal Data of third parties** (e.g. prospects, business partners, clients and customers of the Customer, referred to as 'contacts' and 'companies' in the Tool):
  - First name
  - Last name
  - E-mail address(es)
  - Primary address
  - Telephone number(s) (landline/mobile)
  - Fax
  - Gender
  - Date of birth
  - IBAN and BIC
  - Language
  - Video recordings
  - Other Personal Customer Account Data, depending on the use of the Services by the Customer (e.g. adding of custom fields to enter more Personal Customer Account Data; uploading or providing documents which contain Personal Customer Account Data; entering descriptions of free fields such as in tasks, projects, tickets and time tracking which contain Personal Customer Account Data; etc.)

TEAMLEADER does not, under any circumstances, expect to collect any special categories of Personal Data as defined in the Privacy Legislation, including, but not limited to: information about the Data Subject's health, race, political opinions, religious or other beliefs, sexual orientation, etc. The responsibility for any Processing of such sensitive data through the Customer Account and Services rests entirely with the Customer.

II. Categories of Data Subjects

- Users;
- Prospects of the Customer;
- Customers of the Customer;
- Suppliers of the Customer;
- Business partners of the Customer;
- Service providers of the Customer;
- Other Data Subjects whose Personal Data are entered into the Tool by Users.

III. The use of Personal Data, means and purposes of Processing

- Use of Personal Data:

- Make the Personal Customer Account Data readily available, editable, exportable and analyzable for the Customer in the Customer Account;
- Store the Personal Customer Account Data in the cloud;
- Make back-ups of the Personal Customer Account Data for disaster recovery purposes.

[1] The Customer acknowledges that the summary, as mentioned above, provides a general overview of the Personal Customer Account Data which TEAMLEADER expects to Process in the context of the Agreement. TEAMLEADER may also Process certain additional Personal Customer Account Data it receives from providers of Optional Integrations selected by the Customer. The Personal Customer Account Data TEAMLEADER expects to Process as well as the purposes of Processing depend on the concrete Optional Integration. For the sake of clarity, this overview does not cover all possible situations.

- Means of Processing:

- The Tool;
- The Standard Integrations.

- Purposes of Processing:

- Management of tasks, meetings, calls
- Adding of Personal Customer Account Data to the CRM section in order to follow-up sent emails and management of contacts and companies
- Follow-up of sales projects (including quotation management)
- Project planning (including internal projects)
- Management of Users / teams of Users
- Time tracking
- Creation and management of support tickets (including statistics thereof)
- Creation and management of targets
- Invoicing (InvoiceCloud)
- Creating, sending and signing quotations (Cloudsign)
- Voice over IP
- Management of (targeted) mailings
- Creation and management of delivery notes
- Creation and management of orders
- Creation, planning and management of events
- Saving and collecting documents
- Management of stock
- Scheduling and holding video meetings (Lead Capture Booster)

IV. Retention period:

TEAMLEADER shall retain the Personal Customer Account Data as long as the Agreement is ongoing, unless the Customer performs or requests an earlier deletion.

Once the Agreement has ended, TEAMLEADER shall first soft delete any Personal Customer Account Data. TEAMLEADER shall subsequently hard delete the Personal Customer Account Data at the earliest thirty (30) days and at the latest three (3) months after the Agreement has ended.

In some cases, TEAMLEADER will first apply 'soft deletion' before permanently (hard) deleting the Personal Customer Account Data. TEAMLEADER opts for 'soft deletion' in order to be able to reverse potential mistakes/errors made by the Customer and to be able to recover the Personal Customer Account Data and reactivate the Customer Account within 30 days after deactivation thereof.

Upon termination of the Agreement, TEAMLEADER shall be entitled to retain the anonymous and anonymized Customer Account Data (or part thereof) for research, training, educational, statistical and commercial purposes.

Overview II – Description of security measures

This document entails the technical and organizational security measures implemented by Teamleader in support of its (Processing) activities, as set forth by the Privacy Legislation.

I. Access control of Processing areas (Physical)

Web applications, communications and database servers of Teamleader are located in secure data centers in Ireland, which are operated by Amazon Web Services, Inc. with whom TEAMLEADER has signed the 'AWS Data Processing Addendum' in order to be compliant with the standards and obligations as set forth in the Privacy Legislation.

II. Access control to Personal Data Processing systems (logical)

TEAMLEADER has implemented suitable measures to prevent its Personal Customer Account Data Processing systems from being used by unauthorized persons.

This is accomplished by:

- Establishing the identification of the terminal and/or the terminal user to the TEAMLEADER systems;
- Automatic time-out of user terminal if left idle. Identification and password required to reopen;
- Automatic lock out of the user ID when several erroneous passwords are entered. Events are logged and logs are reviewed on a regular basis;
- Utilizing firewall, router and VPN-based access controls to protect the private service networks and back-end-servers;
- Ad hoc monitoring infrastructure security;
- Regularly examining security risks by internal employees and third party auditors;
- Issuing and safeguarding of identification codes;
- Role-based access control implemented in a manner consistent with principle of least privilege;
- Access to host servers, applications, databases, routers, switches, etc. is logged;
- Making use of commercial and custom tools to collect and examine the Tool and system logs for anomalies.

III. Availability control

TEAMLEADER has implemented suitable measures to ensure that Personal Customer Account Data is protected from accidental destruction or loss.

This is accomplished by:

- Redundant service infrastructure;
- Constantly evaluating data centers and Internet service providers (ISPs) to optimize performance for its customers in regards to bandwidth, latency and disaster recovery isolation;
- Situating data centers in secure co-location facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy;
- Service level agreements from ISPs to ensure a high level of uptime;
- Rapid failover capability.

IV. Transmission control

TEAMLEADER has implemented suitable measures to prevent Personal Customer Account Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media.

This is accomplished by:

- Use of adequate firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- Personal Customer Account Data is encrypted during transmission using up to date versions of TLS or other security protocols using strong encryption algorithms and keys;
- Protecting web-based access to account management interfaces by employees through encrypted TLS
- End-to-end encryption of screen sharing for remote access, support, or real time communication.

V. Input control

TEAMLEADER has implemented suitable measures to ensure that it is possible to check and establish whether and by whom Personal Customer Account Data have been input into Personal Data Processing systems or removed.

This is accomplished by:

- Authentication of the authorized personnel;
- Protective measures for Personal Customer Account Data input into memory, as well as for the reading, alteration and deletion of stored Personal Customer Account Data, including by documenting or logging material changes to account data or account settings;
- Segregation and protection of all stored Personal Customer Account Data via database schemas, logical access controls, and/or encryption;
- Utilization of user identification credentials;
- Physical security of data Processing facilities;
- Session timeouts.

VI. Monitoring

TEAMLEADER does not access Personal Customer Account Data, except:

- To provide the required Services under the Agreement;
- To do security checks;
- To provide assistance to the Customer;
- To do usage research and statistical analysis;
- As required by law; or
- Upon request of the Customer.

This is accomplished by:

- Individual appointment of system administrators;
- A strict access control policy which provides for access rights in proportion to the employee's role;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure.