# DATA PROCESSING AGREEMENT

## BETWEEN:

**1/** Limited company (naamloze vennootschap) "**TEAMLEADER**", with its registered office at 9000 Ghent, Dok-Noord 3A, Belgium, VAT BE-0899.623.035, RPR/RPM Ghent, division Ghent, hereby duly represented by its managing director Jeroen De Wit;

**2/** The Customer

Hereinafter referred to as "**Teamleader"**

Hereinafter collectively referred to as the "**Parties**" and individually as a "**Party**".

## CONSIDERATIONS

Within the context of the performance of certain activities and 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 Belgian Privacy Act of 8 December 1992 regarding the protection of privacy in relation to the processing of personal data, **(ii)** 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 and repealing Directive 95/46/EC') and/or and **(iii)** all (future) Belgian laws regarding the implementation of this Regulation. (hereinafter referred to as the **"Privacy Legislation")**.

Through this agreement 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.

## THEREFORE, PARTIES HAVE AGREED AS FOLLOWS

### 1 DEFINITIONS

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

**Assignment:** All activities, performed by Teamleader for the Customer, and any other form of cooperation whereby Teamleader Processes Personal Data for the Customer, regardless of the legal nature of the agreement under which this Processing takes place;

**Controller:** The entity, which determines the purposes and means of the Processing of Personal Data;

**Data Subject:** A natural person to whom the Personal Data relates;

**Data Breach:** Unauthorized disclosure, access, abuse, loss, theft or accidental or unlawful destruction of Personal Data, which are processed by Teamleader on behalf of the Customer;

**Personal Data**: Any information relating to an identified or identifiable natural person;

**Platform:** The online application of Teamleader with the brand name "Teamleader®" (trademark registration number 012661963), which offers an integration of various services that ensure a more efficient business administration of its customers. The online services facilitate among others online management and cooperation, and consist among other things of a CRM system, agenda, quotation management, API, project planning module, invoicing module, ticketing and Voice-over-IP;

**Processor**: The entity which Processes Personal Data on behalf of the Controller;

**Process/Processing:** Any operation or set of operations which is performed upon Personal Data or sets of Personal Data, including, but not limited to: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data;

**Services:** All services, provided by Teamleader to the Customer with respect to the Platform (such as but no limited to support, webinars, e-books);

**Sub-processor:** Any Processor engaged by Teamleader.

The agreement includes the following annexes:

**Annex 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;

**Annex II:** Overview and description of the security measures taken by Teamleader under this agreement.

### 2 ROLES OF THE PARTIES

Parties acknowledge and agree that with regard to the Processing of Personal 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 PLATFORM AND/OR THE SERVICES

**3.1** The Customer acknowledges explicitly that:

- ✓ Teamleader purely acts as a facilitator of the Platform and/or the Services. Hence, the Customer shall be solely responsible on how it makes use of the Platform and/or the Services;
- ✓ As a result of the use of the Platform, a number of integrations shall automatically be made through the application programming interface ('API'). All other integrations offered by Teamleader are optional and shall only be made upon explicit request of the Customer;
- ✓ It shall be solely responsible to comply with all laws and regulations (such as but not limited to the retention period) imposed on it by making use of the Platform and/or the Services.

**3.2** In case of misuse by the Customer of the Platform and/or 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** Customer acknowledges that as a consequence of making use of the Platform and the Services of Teamleader, the latter shall Process Personal Data as collected by the Customer.

**4.2** Teamleader shall Process the Personal 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 Assignment – provide all its know-how in order to perform the Assignment according to the rules of art, as it fits a specialized and 'good' processor.

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

**4.4** The Customer, as Controller, owns and retains full control concerning (i) the Processing of Personal Data, (ii), the types of Personal 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 Data, entered into the Platform, and the means by which it acquired such Personal Data.

The responsibility and control concerning the Personal Data, subject to this Agreement, 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 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 Data, as set forth in **Annex II**.

## 6 SUB-PROCESSORS

**6.1** The Customer acknowledges and agrees that Teamleader may engage third-party Sub-processors in connection with the Assignment. In such case, Teamleader shall ensure that the Sub-processors are at least bound by the same obligations by which Teamleader is bound under this agreement.

**6.2** Teamleader undertakes to make two (2) lists available on its Platform concerning the Sub-processors on which it appeals for the performance of the Assignment:

- ✓ A list of Sub-processors on which Teamleader always appeals since these integrations are standard (cfr. **Article 3.1**);
- ✓ A list of optional Sub-processors on which Teamleader solely appeals if the Customer has selected these integrations (cfr. **Article 3.1**).

Such list shall include the identities of those Sub-processors and their country of location.

**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).

**6.4** Without prejudice to **Article 6.3**, the Customer is entitled to oppose against a new Sub-processor appointed by Teamleader in case it concerns a Sub-Processor of a standard integration.

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**).

**6.5** In the event the Customer objects to a new Sub-processor and such objection is not found unreasonable, Teamleader will use reasonable efforts to (i) make available to the Customer a change in the Platform and/or the Services or (ii) recommend a commercially reasonable change to the Customer's configuration or use of the Platform and/or the Services to avoid Processing of Personal Data by the objected new Sub-processor without unreasonably burdening the Customer.

If Teamleader is, however, unable to make available such change within a reasonable period of time (which shall not exceed thirty (30) days following the objection of the Customer), the Customer may terminate the agreement with Teamleader on the condition that:

- ✓ The Platform 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 DATA OUTSIDE THE EEA

Any transfer of Personal 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 as published in the Decision of the European Commission of February 5, 2010 (Decision 2010/87/EC) 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 Data confidential and thus not disclose nor transfer any Personal Data to third parties, without the prior written agreement of the Customer, unless when:

- ✓ Explicit written deviation from this agreement;
- ✓ 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 Assignment, are informed of the confidential nature of the Personal 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 Data is limited to such personnel performing the Assignment in accordance with the agreement.

## 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 Data;
- ✓ Has the intention to disclose Personal Data to a competent public authority;
- ✓ Determines or reasonably suspects a Data Breach has occurred in relation to the Personal 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 Platform and/or the Services – does not have the ability to correct, amend, block or delete Personal 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 Platform and/or 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 PERSONAL DATA**

**12.1** Upon termination of the Assignment and/or termination of the agreement, Teamleader shall notify the Customer that it has the possibility during a term, as mentioned in such notification, to export the Personal Data from the Platform through the available export tools.

**12.2** Once the aforementioned term regarding export has passed, Teamleader shall first delete the Personal Data via 'soft deletion' and subsequently, once a term of six (6) months has passed, anonymize the Personal Data.

**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 agreement.

**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.

**14 MISCELLANEOUS**

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

**14.2** If one or more provisions of this agreement are found to be invalid, illegal or unenforceable, in whole or in part, the remainder of that provision and of this agreement shall remain in full force and effect as if such invalid, illegal or unenforceable provision had never been contained herein. Moreover, in such event, Parties shall negotiate to replace the invalid provision by an equivalent provision in accordance with the spirit of this agreement. 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 agreement shall only be valid and binding to the extent that they have been accepted in writing by both Parties.

**14.4** This agreement 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 agreement, can only be regarded as a toleration of a certain state, and does not lead to forfeiture

**14.6** This agreement prevails to any other agreement 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 agreement 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 agreement shall be submitted to the exclusive jurisdiction of the courts of Teamleader's registered office.

******

**ANNEXES:**

- Annex I – Overview of Personal Data
- Annex II – Description of security measures

## Annex I – Overview of Personal Data[1]

**I. Overview of the Personal Data, which Parties expect to Process**

- Name
- First name
- User account
- Password
- E-mail
- Telephone number (land line/mobile)
- Home address
- Bank account number
- Bank code
- Other Personal Data, depending on the free fields added by the Customer

**II. The categories of Data Subjects whose Personal Data shall be Processed:**

- Employees
- Prospects
- Customers
- Suppliers
- Business partners
- Service providers
- Other

**III. The use (= way(s) of Processing) of Personal Data and the means and purposes of Processing:**

**Use of Personal Data:**

- Retention in the Platform and/or the app
- Processing

**Means of Processing:**

- Through Teamleader's developed software
- Integrations:
  - Standard integrations
  - Integrations selected by the Customer

**Purpose of Processing:**

- Standard integrations
  - Management of tasks, meetings, calls
  - Adding Personal Data to the CRM-tool in order to follow-up sent emails and management of contacts and companies
  - Follow-up sales project (incl. quotation management)
  - Projectplanning (incl. internal projects)
  - Invoicing
  - Management of users / teams of users of the Platform
  - Time tracking
  - Creation and management of support tickets (incl. statistics thereof)

[1] The Customer acknowledges that the summary, as mentioned above, provides a general overview of the Personal Data, which Teamleader may Process through its Platform. In case the Platform is customized following a request of the Customer (through integrations available on the Marketplace), Teamleader can upon explicit request from the Customer provide a customized/updated overview resp. make it available on the Platform.

- Creation and management of targets
- 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
- Creation of Teamleader accounts by the Customer
- Management of stock

- Integrations selected by the Customer (the purpose of Processing of such integrations shall depend on the integrations selected)

**IV. The term(s) during which the (different types of) Personal Data shall be stored:**

Teamleader shall retain the Personal Data as long as the Assignment and/or the agreement is ongoing. Once the Assignment and/or the agreement has been terminated and the period of export by the Customer has expired, Teamleader shall first delete the Personal Data via 'soft deletion' and subsequently, once a term of six (6) months has passed, anonymize the Personal Data.

Notwithstanding this standard rule, Teamleader shall – if required – apply a shorter retention period and consequently delete the concerned Personal Data via 'soft deletion'. In any event, such 'soft deletion' shall always be followed by anonymization upon termination of the Assignment and/or agreement (as described above).

Teamleader opts for 'soft deletion' to deal with, such as but not limited to, mistakes/errors from the Customer and reactivation of the Teamleader account upon termination thereof.

Upon termination of the Assignment and/or the agreement, Teamleader shall also be entitled to retain the anonymized Personal Data (or part thereof) for statistical and analytical reasons.

## Annex 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 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 its Platform and system logs for anomalies.

**III. Availability Control**

Teamleader has implemented suitable measures to ensure that Personal 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 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;
- Sensitive Personal 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 Data have been input into Personal Data Processing systems or removed.

This is accomplished by:

- Authentication of the authorized personnel;
- Protective measures for Personal Data input into memory, as well as for the reading, alteration and deletion of stored Personal Data, including by documenting or logging material changes to account data or account settings;
- Segregation and protection of all stored Personal 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 Data of the Customer, except:

- To provide the required services under the agreement with the Customer;
- In support of its customer experience;
- As required by law; or
- Upon request of the Customer.

This is accomplished by:

- Individual appointment of system administrators;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure.