



Data Processing Agreements ("DPA")

Version: 1.2dh (Sep 19th, 2023) / ID: JZUD1134

Data Processing Agreements ("DPA") between:

Company	Local Contexts
Represented by	Signee of Local Contexts
Street	1178 Broadway, Fl 2, PMB 2007
Postal code / City	US - 10001 New York
Country	United States

hereinafter referred to as "Data Controller"

Company	Zammad GmbH
Represented by	Martin Edenhofer, CEO
Street	Marienstraße 18
Postal code / City	D-10117 Berlin
Land	Germany

hereinafter referred to as "Data Processor"



§ 1 Preamble, scope, definition

- 1.1 This DPA governs the right and duties of the Parties regarding the processing of personal data ("processing activities").
- 1.2 This DPA applies to all data processing activities of the Data Processor, its employees or sub-processors.
- 1.3 All Definitions shall be construed as defined in Art. 4 General Data Protection Regulations ("GDPR"). The words "in written" shall have the meaning as defined in § 126 BGB ("German Civil Code"). Therefore, the original signature of the representative under the document is required or an electronic signature as described in the Regulation EU 910/214 (eIDAS) and the Vertrauensdienstegesetz ("VDG"). All other documents and notices shall be valid in text form, subject to providing sufficient proof of its authenticity.

§ 2 Subject matter and term of the processing activities

- 2.1 The Data Processor provides the following processing activities for the Data Controller:
 - a) Storing of data on behalf of the Data Controller.
 - b) All other possible processing activities, like usage, alteration or deletion are subject to a support case and prior assignment by the Data Controller.
 - c) All processing activities are subject to the Terms and Conditions ("T&C") of the Data Processor for the Zammad Hosted Version, which constitutes the Service Agreement between the Parties, as attached to this DPA and can be downloaded via <https://zammad.com/terms>.
- 2.2 This DPA is effective as from 15.03.2023 and shall continue for an indefinite period, ending with termination of the DPA and the Service Agreement by either of the Parties.
- 2.3 The data processing activities may include: Storage, adaptation or alteration, usage for purpose of support case, and deletion upon request.
- 2.4 The data processing activities serve the purpose of: Providing a platform for data processing on behalf of the Data Controller.
- 2.5 The following categories of personal data are processed:
 - a) Personal data, which might be contained in questions by customers of the Data Controller to experts, like(eg. Names, email addresses).
 - b) Customer details: Contact information like Email addresses and names as well as other personal data provided by the customer.
- 2.6 The following categories of data subjects are affected:
 - a) Registered employees and directors of the Data Controller
 - b) Customers of the Data Controller (Enduser)
 - c) Experts

§ 3 Duties of the Data Processor

- 3.1 The Data Processor warrants to process the data received only for the purposes contractual agreed upon or legally obliged by law. No other data processing activities shall be conducted.
- 3.2 The Data Processor warrants that it is aware of all data protection regulations applicable to the processing activities and that it will adhere to the principles relating to processing of personal data and that all processing shall be conducted lawful.
- 3.3 The Data Processor warrants that all processing activities shall be conducted in a confidential manner.
- 3.4 The Data Processor warrants that all its employees, consultants and sub-processors are bound to secrecy and confidentiality, either by contract or law.
- 3.5 The Data Processor agrees, that every person employed by it, was made aware of the relevant legal and contractual data protection requirements before the commencement of any processing activities and will be trained accordingly on a regular base.
- 3.6 The Data Processor has a duty of care to ensure that every person employed by it conducting data processing activities is instructed and supervised in accordance with the requirements of legal and contractual data protection requirements.
- 3.7 The Data Processor shall maintain and constantly update a record of data processing activities. The record of data processing activities has to be made available to the Data Controller in its latest version. Further, upon request by the Data Controller, the Data Processor will immediately provide all information necessary for the Data Controller in order to establish and maintain its own record of data processing activities.
- 3.8 The Data Processor shall allow the Data Controller, or any person authorized by it, to audit the Data Processors compliance with all relevant data protection regulations and the terms of this DPA, in particular by requesting information and access to the processed data and data processing programs, as well as inspections of the Data Processors premises on reasonable notice and during business hours. The Data Processor agrees to provide access to all files, document and premises, subject to access being reasonably necessary for such audit.



- 3.9 In the event of an audit of the Data Controller by the supervising authority, or upon lawful request of the data subject, the Data Processor shall assist the Data Controller to a reasonable extent, subject to the audit or request being related to the processing activities covered by this DPA.
- 3.10 The Data Processor must refrain from providing any information with regard to the processing activities covered by this DPA, to any third party without the written consent of the Data Controller. Any requests directed towards the Data Processor must be transmitted to the Data Controller without undue delay.
- 3.11 The Processing is carried out within the EU or the EEA. Any relocation to a third country is subject to the requirements of chapter 5 of the GDPR and this DPA.
- 3.12 The Data Processor shall designate a competent and reliable data protection officer. There shall be no conflicts of interest. The Data Processor shall give notice to the Data Controller of any changes of the person or responsibilities of the data protection officer without undue delay.

§ 4 Technical and organizational security measures

- 4.1 The Data Processor warrants to uphold the security measures as described in Annex 2 of this DPA, as a minimum requirement for data protection.
- 4.2 All technical and organizational security measures may be adjusted to technical and legal developments, subject to maintaining the level of security provided in this DPA. The Data Processor shall notify the Data Controller of any adjustments without undue delay. Material deviations from the level of security set out in this DPA must be agreed upon by the parties prior to implementation.
- 4.3 The Data Processor shall give notice to the Data Controller of any deviations from the level of security set out in this DPA without undue delay.
- 4.4 The Data Processor warrants that all data processed during the course of the processing activities shall be stored separately of all other data stored by the Data Processor.
- 4.5 The Data Processor warrants not to create any copies of the data provided by the Data Controller without its consent, except for those temporary necessary for the performance of the Service Agreement. Any copies are subject to the security measures set out in this DPA.
- 4.6 Any data processing activities on private premises are subject to prior written consent by the Data Controller. The Data Processor shall ensure by contractual agreement with its employees or sub-processors that all security measures set out in this DPA are adhered to and that access for audits is provided. No data processing activities on private electronics shall be permitted.
- 4.7 The Data Processor shall label all data storage mediums, which are used for the processing activities on behalf of the Data Processor accordingly. Further they shall be stored securely and accessible only by authorized persons. Further, any change in location shall be documented by the Data Processor.
- 4.8 The Data Processor shall document its compliance with data protection regulations and the requirements established in this DPA on a regular base ("documentation"). It shall provide such documentation to the Data Controller either upon request or latest every 12 months. Documentation may be provided by approved certification or code of conduct.

§ 5 Rules about rectification, erasure, interlocking of personal data

- 5.1 The Data Processor shall rectify, erase or interlock personal data in accordance with this DPA, the Service Agreement and on documented instructions of the Data Controller only.
- 5.2 At any time, the Data Processor shall carry out the documented instructions of the Data Controller with regard to clause 5.1. of this DPA.

§ 6 Sub-processing

- 6.1 The Data Processor shall not engage another processor (sub-processor) without prior specific or general written authorization of the Data Controller.
- 6.2 Where a processor engages a sub-processor for specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in this DPA or the Service Agreement shall be imposed on the sub-processor by way of a contract. This includes the provisions of this Paragraph.
- 6.3 For the purpose of sub-processing, the Data Controller shall have all rights against the sub-processor, it has in relation to the Data Processor. The sub-processor shall allow for and contribute to audits, including inspections, conducted by the Data Controller or a third party authorized by the Data Controller.
- 6.4 The responsibilities regarding the processing activities of the Data Processor and its sub-processor shall be separated. The same shall apply between multiple sub-processors.
- 6.5 The sub-processor must not engage further sub-processors.



- 6.6 The Data Processor has a duty of care to ensure that any sub-processor is chosen based on its appropriate technical and organizational measures.
- 6.7 The Data Processor warrants not to transfer any personal data to the sub-processor before making available to the Data Controller all information necessary to demonstrate the sub-processor's compliance with the obligations set out in this DPA. Such documentation must be provided to the Data Controller without undue delay.
- 6.8 Any engagement of a sub-processor located outside of the EU or EEA is subject to the requirements set out in Chapter V of the GDPR. The Data Processor shall use only sub-processors providing sufficient guarantees to implement appropriate technical and organizational measures. The Data Processor shall inform the Data Controller of the details of such guarantees and the manner in which those can be verified.
- 6.9 The Data Processor shall appropriately audit the sub-processor's compliance with this DPA and the requirements set out in the GDPR on a regular base, latest every 12 months. The audit shall be documented and submitted to the Data Controller without undue delay.
- 6.10 The Data Processor will indemnify the Data Controller for any damages arising out of any failure of its sub-processor to comply with this DPA or the requirements of the GDPR with regard to the processing activities.
- 6.11 Currently the Data Processor engages the sub-processors listed in Appendix 3 to this DPA (name, address, services) with the data processing activities described. The Data Controller consents to the processing activities by the listed sub-processors to the extent described in Appendix 3 and subject to the terms set out in this DPA.
- 6.12 For the purpose of this DPA, sub-processing is limited to processing activities connected to the services rendered within the Service Agreement. Notwithstanding that all ancillary services, like transport, maintenance and cleaning services, as well as telecommunication services and user support are not deemed to be sub-processing activities for the purposes of this DPA, the Data Processor shall uphold all requirements of data protection regulations in relation to those service providers.

§ 7 Rights and duties of the Data Controller

- 7.1 The Data Controller shall be responsible for the assessment of the lawfulness of the processing activities and the observance of the rights of the data subject.
- 7.2 All orders, partial orders or instructions by the Data Controller shall be documented, except for emergency situations, in which verbal instructions shall suffice. The Data Controller shall provide for documentation of the instruction without undue delay.
- 7.3 The Data Controller shall notify the Data Processor without undue delay after becoming aware of errors or irregularities in the results of the services rendered by the Data Processor.

§ 8 Notification

- 8.1 The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach, or reasonable suspicion of such. The notification shall at least comply with the requirements set out in Art. 33 (3) GDPR.
- 8.2 The Data Processor shall notify the Data Controller without undue delay after becoming aware of any disturbances of the processing activities and any breaches of its employees of this DPA or data protection regulations.
- 8.3 The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Articles 15, 32 to 36 taking into account the nature of processing and the information available to the Data Processor.

§ 9 Instructions

- 9.1 All data processing activities shall be conducted only on documented instructions of the Data Controller.
- 9.2 The Data Controller and the Data Processor shall give or receive instructions only through the persons authorized and listed in Appendix 4.
- 9.3 The Parties shall inform each other without undue delay, in the event of a change of the authorized person or the person becoming unable to perform his or her duty.
- 9.4 The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes this DPA or other data protection regulations. In the event of a serious infringement by the Data Controller, the Data Processor has the right to terminate this DPA and the Service Agreement immediately. This includes instructions which are in obvious violation of the data protection regulations.

§ 10 Termination of the DPA and the Service Agreement

- 10.1 Upon termination of this DPA and the Service Agreement or upon the request of the Data Controller, the Data Processor shall, depending on the choice of the Data Controller, delete all the personal data or return it to the Data Controller. This includes the deletion of all copies, unless EU Regulations or German State law requires storage of the personal data for a limited time. The deletion shall be conducted in a manner that does not allow for restoration with reasonable efforts.



- 10.2 The Data Processor is responsible to instruct its sub-processors immediately about the duty to delete and its compliance with the instruction.
- 10.3 The Data Processor shall provide proof of proper deletion without undue delay.
- 10.4 The Data Processor shall store documentation of proper deletion beyond the term of the DPA and the Service Agreement in accordance with any legal requirements. Upon expiration or termination of this DPA and the Service Agreement the Data Processor may hand over such documentation to the Data Controller in order to discharge its legal duties.

§ 11 Compensation

- 11.1 The Compensation is subject to the terms of the Service Agreement. This DPA shall convey no right for a separate remuneration or reimbursement.

§ 12 Liability

- 12.1 The Parties shall be jointly and severally liable to the data subjects for any damages, which result from a breach of data protection regulations in regard to the data processing activities.
- 12.2 The Data Processor shall carry the burden of proof that it is not responsible for the damages, provided that the damages are connected to the data processed within the processing activities. The Data Processor shall indemnify the Data Controller of any reasonable claims related to the processing activities, if the Data Processor is unable to discharge this burden.
- 12.3 The Data Processor shall be liable for any loss or damages arising or resulting from any incompliance of its employees, sub-processors or other third parties engaged in the performance of its duties under the DPA or the Service Agreement.

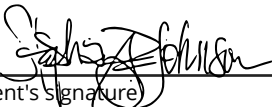
§ 13 Exceptional right of termination

- 13.1 The Data Controller shall be entitled to terminate this DPA without a notice period (exceptional right of termination) in the event of the Data Processor committing a serious breach of this DPA or data protection regulations, the Data Processors inability or unwillingness to follow instructions or the Data Processors unwillingness to conduct necessary and appropriate audits.
- 13.2 In the event of the Data Controller detecting a substantial incompliance with the provisions of this DPA during an audit, in particular a serious deviation from the required level of security, this shall be deemed a serious breach of this DPA.
- 13.3 In the event of minor breaches of this DPA, the Data Controller shall give the Data Processor an adequate period of time to rectify such breach. The Data Controller shall be entitled to terminates this DPA without a notice period if the Data Processor is unable or unwilling to rectify the breach within the deadline.
- 13.4 There shall be no reimbursement of costs within the meaning of § 628 (2) German Civil Code ("BGB").

§ 14 Miscellaneous

- 14.1 Both Parties shall treat all information received during the course of the processing activities and thereafter with strict confidentiality. In doubt the parties shall require each other's written consent with regard to the usage of the information.
- 14.2 Should the property of the Data Controller be endangered by any acts of third parties (such as seizure or confiscation), by insolvency, settlement proceedings or by other comparable events, the Data Controller shall give notice to the Data Controller without undue delay.
- 14.3 Additional oral agreements do not exist. Any additional terms or supplementary arrangements shall not be valid unless made in writing. The same applies to this provision.
- 14.4 The right of retention within the meaning of § 273 BGB shall not apply in regard to the processed personal data and the related data storage devices.
- 14.5 In case one provision of this DPA is invalid, the validity of the remaining provisions shall not be affected thereby.


Place, date



Client's signature

Berlin, 14. March 2024

Place, date



Contractor's signature (Martin Edenhofer)



Annex 1 - Certification

The hosting of the instances by Zammad GmbH takes place in ISO 27001 certified data centers of myLoc managed IT AG, Am Gatherhof 44, D-40472 Düsseldorf Germany or Hetzner Online GmbH, Industriestrasse 25, D-91710 Gunzenhausen. The scope of certification includes a "Tested Data Center Management" according to ISO 27001:2013.

The last certification of Hetzner Online GmbH was carried out according to the certificate (certificate no. ZN-2022-22) in September 2022 and is valid for three years. A duplicate of the certification is attached.



FOX
Certification

ZERTIFIKAT

HETZNER

FOX Certification GmbH bescheinigt hiermit, dass das Informationssicherheitsmanagementsystem des Antragstellers

Hetzner Online GmbH
Industriestraße 25
D-91710 Gunzenhausen

im Geltungsbereich

"Der Anwendungsbereich des Informationssicherheitsmanagementsystems umfasst alle Hosting-Dienstleistungen und die Rechenzentren der Hetzner Online GmbH."

auf Grundlage des Statement of Applicability in der Version 3.0 die Anforderungen des folgenden Regelwerks erfüllt:

ISO/IEC 27001:2013

Im Zertifizierungsaudit konnten Nachweise vorgelegt werden, die die Erfüllung der Anforderungen belegen. In das Managementsystem sind folgende Standorte einbezogen:

Hetzner Online GmbH
Sigmundstraße 135
90431 Nürnberg
Deutschland

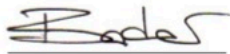
Hetzner Online GmbH
Am Datacenter-Park 1
08223 Falkenstein/Vogtland
Deutschland

Hetzner Online GmbH
Huurrekuja 10
04360 Tuusula
Finland

Statement of Applicability(SoA):
Zertifizierungsentscheidung:
Ausgestellt am:
Gültigkeit Zertifikat:
Zertifikatsnummer:

Version 3.00
23.09.2022
23.09.2022
27.09.2022 - 26.09.2025
ZN-2022-22 v.1.2

FOX Certification GmbH
Graf-Dürkheim-Straße 3
87642 Halblech


Zertifizierungsstelle



Seite 1/2

The last certification of myLoc managed IT AG was carried out according to the certificate (certificate no. DC00511) in August 2021 and is valid for three years. A corresponding duplicate of the certification is attached.

7/13

Zammad GmbH
Marienstraße 18
10117 Berlin
Germany

Phone:
+49 (0) 30 55 57 160-0
Fax:
+49 (0) 30 55 57 160-99

Email:
info@zammad.com
Web:
http://zammad.com

Bank Account:
Berliner Bank
IBAN: DE62100708480634993000
SWIFT/BIC: DEUTDEDB110

Managing Director:
Martin Edenhofer
Local Court:
Berlin-Charlottenburg
HRB 163946 B
VATID: DE298516802



ZERTIFIKAT

Das Informationssicherheitsmanagementsystem von

myLoc managed IT AG
Am Gatherhof 44 | 40472 Düsseldorf | Deutschland



wurde auditiert und hat den Nachweis erbracht, dass die Anforderungen folgender Norm erfüllt werden:

DIN ISO/IEC 27001:2017

Geltungsbereich der Zertifizierung:

Der Geltungsbereich erstreckt sich auf die Dienstleistungen Colocation, Managed Hosting, Server Hosting und Cloud Hosting im Geschäftskundensegment an den Standorten:
Am Gatherhof 44, 40472 Düsseldorf
In der Steele 2, 40599 Düsseldorf

Version zur Erklärung der Anwendbarkeit: 16.06.2021 6.0

Dieses Zertifikat ist gültig vom 06.08.2021 bis 05.08.2024

Ausstellungsdatum: 06.08.2021

Zertifikat Nr. DC00511

Dies ist ein Gruppenzertifikat.
Der Anhang ist Bestandteil dieser Urkunde.

Dipl. Wirtsch.-Ing. (FH) Thorsten Greiner, Managing Director
TÜV® Saarland Certification GmbH
Am TÜV 1 | 66280 Sulzbach/Saar | Germany
T +49 (0) 68 97 506 0 | cert@tuv-saar.com



Seite 1 von 2

DE/A/213849
TÜV®



Anhang

zu Zertifikat Nr. DC00511

Standort:

myLoc managed IT AG
In der Steele 2 | 40599 Düsseldorf | Deutschland



Seite 2 von 2

DE/A/213711
TÜV®

9/13

Zammad GmbH
Marienstraße 18
10117 Berlin
Germany

Phone:
+49 (0) 30 55 57 160-0
Fax:
+49 (0) 30 55 57 160-99

Email:
info@zammad.com
Web:
http://zammad.com

Bank Account:
Berliner Bank
IBAN: DE62100708480634993000
SWIFT/BIC: DEUTDEDB110

Managing Director:
Martin Edenhofer
Local Court:
Berlin-Charlottenburg
HRB 163946 B
VATID: DE298516802



Annex 2 - TOM

	Controlling objectives	Technical and organizational security measures
1	Access/ Entry (to rooms and buildings) Only authorized persons have access to data-processing equipment with which personal data is processed.	<ul style="list-style-type: none"> • No access without an appointment • Access secured by locking system • Offices locked in after hour
2	Access (to IT-system, Applications) Only authorized persons have access to data-processing systems with which personal data are processed.	<ul style="list-style-type: none"> • User administration in place • User administration is carried out via a central user control system • Incorrect access attempts are documented
3	Access (to data) It must be ensured that those authorized to use a data processing system can only access the data subject to their level of authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and storage.	<ul style="list-style-type: none"> • Access to the data processing systems is only possible with a valid user account • User accounts, are managed through the central user administration • Access to the central ticket system in which the data is stored is still secured by a group and role concept (read, write, note, move)
4	Input (in data processing systems) It must be ensured that it can be subsequently reviewed and detected whether and by whom personal data has been entered into, modified within or removed from the data processing systems.	<ul style="list-style-type: none"> • Data is only entered in the central ticket system. • Access is secured by a group and role concept. (read, write, note, move) • User administration is carried out via central user control
5	Transfer (of data) It is to be guaranteed that personal data are not read, copied, changed or removed without authorization during electronic transmission or during their transport or storage on data storage devices, and that the recipient can be determined	<ul style="list-style-type: none"> • Personal data are not transferred
6	Availability/ Recovery (of data) It must be ensured that personal data is protected against accidental destruction or loss.	<ul style="list-style-type: none"> • Regular, encrypted and redundant backups are created of all systems • Restoration of the operating status is possible with the previously created backups
7	Data separation (purpose related) It must be ensured that data collected for different purposes can be processed separately.	<ul style="list-style-type: none"> • Direct customer and client assignment of all data ensures that no mixture of data can occur.
8	Pseudonymization It should be possible to pseudonymize individual customer attributes of complete data sets	<ul style="list-style-type: none"> • The pseudonymization of customer attributes can be carried out by the Data Processor according to the Data Controllers specifications.
9	Efficacy The effectiveness of the above security measures must be regularly reviewed and ensured	<ul style="list-style-type: none"> • Performance automated penetration tests • Recording and evaluation of all incidents, with a separate identification, within the internal ticket system • Regular analysis of incidents performed by data protection officers with the management
10	Data processing (when using sub-processors) The Data Processor must ensure that any sub-processors are used by the Data Processor, comply with instructions of the Data Controller and uphold the same level of security as the Data Processor	<ul style="list-style-type: none"> • All sup-processors listed in Annex 3 to this DPA comply with the level of security provided within these TOM's and are bound to adhere the instructions of the Data Controller provided through the Data Processor



11	Data integrity Ensuring that stored personal data cannot be damaged by system malfunctions	<ul style="list-style-type: none">• Regular, encrypted and redundant backups are created of all systems• Backups are stored on different locations
12	Reliability Ensuring that all functions of the system are available and any malfunctions that occur are reported	<ul style="list-style-type: none">• Systems that function independently of each other• Automated reporting of malfunctions• Independent check of the most important functions per instance and show active errors in admin interface and via API



Annex 3 - Subcontractor

	Company, Office	Contractual services
1	myLoc managed IT AG, Am Gatherhof 44, D-40472 Düsseldorf	Server hosting
2	Hetzner Online GmbH, Industriestraße 25, D-91710 Gunzenhausen	Server hosting



Annex 4 - Instructions to authorized persons only

	Contractor	Contractee
1	Martin Edenhofer	
2	Christian Wally	
3		
4		
5		
6		