

Data Processing Addendum

Last updated: 24.04.2026

1. Preamble

Cofinity-X is the first operator of the Catena-X dataspace, enabling secure, sovereign, decentralized data exchange between participants in the automotive value chain. Cofinity-X provides the technical foundations for companies to exchange data securely while retaining full data sovereignty. In general, Cofinity-X does not store or access end customer data in the provision of its services, but provides the infrastructure and marketplace through which participants exchange data in accordance with Catena-X standards. Although Cofinity-X focuses on business/industrial data, some personal data may be processed indirectly for operational purposes. This Data Processing Addendum shall regulate those cases.

This Data Processing Addendum including all its Annexes (hereinafter referred to as "DPA") is made by and between Cofinity-X GmbH ("Cofinity-X") and Customer, collectively "the Parties," in connection with the services that Cofinity-X provides to the Customer under any of Cofinity-X`s framework agreements or any other written or electronic agreement between the Parties (as applicable) ("Main Contract").

This DPA forms part of the Main Contract and is intended to specifically regulate the associated data protection obligations. The purpose is to ensure that the processing of personal data is carried out in accordance with applicable law and with due respect for the rights and freedoms of individual data subjects.

2. Definitions

The following terms have the meanings set out below and apply throughout this DPA. These definitions are intended to be clear, practical, and consistent with the GDPR. In case of inconsistencies, the definitions in the GDPR should prevail.

2.1. Data Protection Laws

"Data Protection Laws" means all laws and regulations applicable to the processing of Personal Data, including the GDPR, the UK GDPR (where applicable), and any national laws that implement or supplement such legislation.

2.2. Processing

"Processing" means any operation performed on Personal Data, whether automated or not, including collecting, storing, organizing, using, disclosing, or deleting such data.

2.3. Controller

"Controller" means the party that determines the purposes and means of Processing Personal Data.

2.4. Processor

“Processor” means the party that Processes Personal Data on behalf of the Controller and in accordance with the Controller’s instructions.

2.5. Sub-Processor

“Sub-Processor” means any third party appointed by Cofinity-X to carry out specific Processing activities involving Personal Data on behalf of the Controller.

2.6. Data Subject

“Data Subject” means any identified or identifiable natural person whose Personal Data is being Processed.

2.7. Personal Data

“Personal Data” means any information relating to an identified or identifiable natural person, including names, identification numbers, contact details, online identifiers, or any data that can reasonably be linked to an individual.

2.8. Customer Personal Data

“Customer Personal Data” means Personal Data that the Customer provides or makes available to Cofinity-X for Processing in connection with the services described in the Agreement.

2.9. Account Data

“Account Data” means Personal Data collected and Processed by Cofinity-X GmbH as an independent Controller for account creation, billing, authentication, security, and related service-administration purposes.

2.10. Confidential Information

“Confidential Information” means any non-public information disclosed by one party to the other, whether written, oral, electronic, or otherwise, including business information, technical information, and any Personal Data Processed under this Addendum.

2.11. International Transfer

“International Transfer” means any transfer of Personal Data to a country outside the EEA or to an international organization, subject to the requirements of the GDPR.

3. Applicability & Scope

3.1. Customer Personal Data

The parties acknowledge and agree that regarding the processing of Customer Personal Data, Customer may act either as a controller or processor and Cofinity-X is a processor. This DPA will apply only to the extent that Cofinity-X processes, on behalf of Customer, Customer Personal Data to which Applicable Data

Protection Legislation applies. The subject matter of the data processing is the provision of the Services, and the processing will be carried out for the duration of the Main Contract. The details of the processing are described in Section 4 and the relevant Annexes.

3.2. Account Data

For Account Data, Cofinity-X acts as an independent Controller. This may include account registration data; billing and payment data; authentication, security, and access-management data; and service usage necessary for administration and security. Cofinity-X will process Account Data as a controller (a) in order to manage the relationship with Customer; (b) carry out Cofinity-X's core business operations; (c) in order to detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) identity verification; (e) to comply with Cofinity-X's legal or regulatory obligations; and (f) as otherwise permitted under Applicable Data Protection Legislation and in accordance with the Main Contract and the company's Privacy Policy.

Each Party shall independently determine the purposes and legal bases for its Processing of Account Data in accordance with GDPR. The Parties do not act as joint controllers for any Processing under this DPA.

To the extent Cofinity-X processes Customer Personal Data for its own anonymization or analytics purposes where so established in the Main Contract, Cofinity-X acts as an independent Controller for such processing. Such processing does not constitute commissioned processing and is not governed by this DPA.

As Controller, Cofinity-X is responsible for compliance with its own obligations under Data Protection Laws.

4. Cofinity-X as a Processor - Processing Customer Personal Data

4.1 Scope of the Assignment

4.1.1 The provisions of this DPA shall always apply as soon as Cofinity-X obtains access to Customer Personal Data for which the Customer is responsible within the meaning of the data protection regulations within the scope of the Main Contract. In these cases, Cofinity-X processes data on behalf of and according to the instructions of the Customer within the meaning of Article 28 GDPR (Commissioned Processing). The Customer remains the responsible party in the sense of data protection law. In this respect, the Customer is responsible for compliance with all data protection regulations, in particular the GDPR, but also for compliance with the legal claims of data subjects in connection with Customer Personal Data.

4.1.2 Customer Personal Data processing by Cofinity-X shall be carried out in the manner, to the extent and for the purpose as specified in Annex 1 to this DPA; the processing concerns the types of personal data and categories of data subjects designated therein. The duration of the processing shall correspond to the term of the Main Contract.

4.1.3. Customer Personal Data processing by Cofinity-X shall generally take place within the European Union (EU) or in another contracting state of the Agreement on the European Economic Area (EEA). Cofinity-X is nevertheless permitted to process Customer Personal Data outside the EEA in compliance with the provisions of this DPA if it informs the Customer in advance of the location of the data processing and the requirements of Articles 44 - 48 of the GDPR are met or an exception pursuant to Article 49 of the GDPR applies.

4.2. Instruction Authority

4.2.1. Cofinity-X shall process the Customer Personal Data in accordance with the Customer's instructions unless Cofinity-X is required by law to process it otherwise. In the latter case, Cofinity-X shall notify the Customer of such legal requirements prior to processing, unless the relevant law prohibits such notification due to an important public interest.

4.2.2. The instructions of the Customer are in principle conclusively defined and documented in the provisions of the main contract, this DPA and any Annexes. Individual instructions which deviate from the stipulations of this agreement or which impose additional requirements shall require the prior consent of Cofinity-X and shall be carried out in accordance with the amendment procedure stipulated in the Main Contract, in which the instruction shall be documented and the assumption of any additional costs incurred by Cofinity-X as a result thereof shall be borne by the Customer.

4.2.3. Customer must ensure that instructions are as clear and comprehensible as possible. Instructions may not violate European or national law. If an instruction is unclear from Cofinity-X's point of view, Cofinity-X shall immediately notify the Customer thereof in writing or by e-mail and request clarification.

4.2.4. If Cofinity-X is of the opinion that an instruction of the Customer violates this Agreement or the applicable data protection law, it shall be entitled, after notifying the Customer accordingly (e.g. by e-mail or via a ticket system), to suspend the execution of the instruction until the Customer confirms the instruction. The parties agree that the sole responsibility for the processing of the data in accordance with the instruction lies with the Customer.

4.2.5. The Customer shall designate a person or persons as authorized to issue instructions to Cofinity-X in writing. The Customer is entitled to replace the person or persons authorized to give instructions and/or his deputy at any time. However, changes must be notified to Cofinity-X in text form in advance.

4.3. Responsibility of Cofinity-X

4.3.1. The Customer shall be solely responsible for the lawfulness of the processing of the data as well as for the protection of the rights of the data subjects in the relationship between the Parties. Should third parties assert claims against Cofinity-X based on the processing of data in accordance with the Main Contract, the Customer shall indemnify Cofinity-X against all such claims upon first request.

4.3.2. The Customer shall be responsible for providing Cofinity-X with the Customer Personal Data in a timely manner for the performance of services under the Main Contract and shall be responsible for the quality of the data. The Customer shall inform Cofinity-X immediately and in full if it discovers errors or irregularities regarding data protection regulations or its instructions when checking Cofinity-X's order results.

4.3.3. Upon request, the Customer shall provide Cofinity-X with the information referred to in Article 30 para. 2 GDPR, insofar as Cofinity-X does not have it itself.

4.3.4. If Cofinity-X is obliged vis-à-vis a government agency or a person to provide information on the processing of Customers Personal Data or to otherwise cooperate with such agencies, the Customer shall be obliged to support Cofinity-X upon first request in providing such information or in fulfilling other obligations to cooperate.

4.4. Personnel Requirement

In order to fulfill its obligations, Cofinity-X shall exclusively use persons who have committed themselves to confidentiality or are subject to appropriate legal secrecy.

4.5. Security of Processing (Technical and Organizational Measures)

4.5.1. Cofinity-X shall, in accordance with Article 32 GDPR, take any necessary and appropriate technical and organizational measures, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the data processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of protection for the Customer Personal Data that is appropriate to the risk.

4.5.2. The current technical and organizational measures are shown in **Annex 2** to this DPA.

4.5.3. Cofinity-X is permitted to change or adapt technical and organizational measures during the term of the contract as long as they continue to meet the legal requirements.

4.6. Involvement of Subprocessors

4.6.1. Cofinity-X may use involve subprocessors in the processing of Customer Personal Data. Subprocessors within the meaning of this DPA are only those who provide services which have a direct connection with the provision of Cofinity-X's services as per the Main Contract. In particular, service providers who merely provide ancillary services, such as the testing or maintenance of data processing procedures or systems by other bodies, telecommunications services, postal and transport services, user services or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems shall not constitute subprocessors. The subprocessors called in at the time of conclusion of this DPA are shown in **Annex 3**.

4.6.2. Cofinity-X may replace its subprocessors at any time if it ensures that it transfers all data protection obligations under this DPA to the new subprocessor. Cofinity-X shall inform the Customer of each intended new Sub-Processor in writing at least [30] days prior to the engagement of such Sub-Processor. The Customer shall have 14 days from receipt of such notification to raise an objection in accordance with this Section. An objection may only be raised by the Customer for good cause to be proven to Cofinity-X. If the Customer does not raise an objection within 14 days after receipt of the notification, its right of objection regarding the corresponding commissioning shall expire. If the Customer raises an objection, Cofinity-X shall be entitled to terminate the Main Contract and this DPA with a notice period of 3 months.

4.6.3. Cofinity-X shall use subprocessors as subprocessors only to the extent that it is ensured that they meet the requirements of Art. 28 GDPR.

4.6.4. In compliance with the requirements of Section 4.1.4. of this DPA, the provisions of this section also apply if a subprocessor in a third country is involved. In this case, Cofinity-X undertakes to comply with the provisions and requirements of Art. 44 et seq. GDPR. Cofinity-X shall, if necessary, cooperate accordingly in such a case.

4.7. International Transfers

4.7.1. Any transfer of Customer Personal Data to a third country outside the EEA shall be made in compliance with Chapter V GDPR.

4.7.2. Where required, Cofinity-X shall incorporate the EU Standard Contractual Clauses (SCCs) by reference.

4.8. Rights of the Data Subjects

4.8.1. Cofinity-X shall support the Customer with technical and organizational measures within reasonable limits in fulfilling its obligation to respond to requests to exercise the rights of data subjects to which they are entitled.

4.8.2. Insofar as a data subject asserts a request to exercise the rights to which they are entitled directly against Cofinity-X, Cofinity-X shall promptly forward this request to the Customer.

4.8.3. Cofinity-X shall provide the Customer with information about the stored data, the recipients of data to which Cofinity-X passes it on in accordance with the order, and the purpose of the storage, unless the Customer has this information itself or can obtain it itself.

4.8.4. Cofinity-X shall enable the Customer to correct, delete or restrict the further processing of Customer's data within the scope of what is reasonable and necessary against reimbursement of the expenses and costs to be proven incurred by Cofinity-X as a result thereof or, at the request of Cofinity-X, to carry out the correction, blocking or restriction of further processing itself if and to the extent that this is impossible for Cofinity-X itself.

4.8.5. Insofar as the data subject has a right to data portability with respect to the Customer Personal Data pursuant to Art. 20 GDPR, Cofinity-X shall support the Customer within the scope of what is reasonable and necessary in providing the Customer Personal Data in a common and machine-readable format against reimbursement of the expenses and costs to be proven incurred by Cofinity-X as a result, if the Customer cannot procure the data otherwise.

4.9. Notification and Support Obligations of Cofinity-X

4.9.1. If the Customer is subject to a statutory obligation to report or notify a data breach (in particular pursuant to Art. 33, 34 GDPR), Cofinity-X shall inform the Customer without undue delay of any reportable events in its area of responsibility. Cofinity-X shall support the Customer in fulfilling the reporting and notification obligations at the Customer's request within the scope of what is reasonable and necessary against reimbursement of the expenses and costs to be proven incurred by Cofinity-X as a result.

4.9.2. Cofinity-X shall support the Customer to the extent reasonable and necessary against reimbursement of the expenses and costs to be proven incurred by Cofinity-X in connection with any data protection impact assessments to be carried out by the Customer and any subsequent consultations with the supervisory authorities pursuant to Art. 35, 36 GDPR.

4.10. Customer Personal Data Breach Notification

Cofinity-X shall notify Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, providing such information as is reasonably available to Cofinity-X at the time of notification. Cofinity-X shall further support Customer, upon Customer's written request and to the extent reasonably practicable, in meeting its obligations under Articles 33 and 34 GDPR, including by providing additional information as it becomes available to Cofinity-X.

4.11. Return or Deletion of Customer Personal Data

4.11.1. Upon termination of the Main Contract, Cofinity-X shall delete Customer Personal Data, or return Customer Personal Data to Customer, unless applicable EU or Member State law requires storage.

4.11.2. Documentation that serves as proof of the proper processing of Customer Personal Data in accordance with the order may be retained by Cofinity-X even after the end of the contract.

4.12. Inspections and Controls

4.12.1. Cofinity-X shall provide the Customer, upon the Customer's request, with all information necessary and available to Cofinity-X to demonstrate compliance with its obligations under this DPA.

4.12.2. The Customer shall be entitled to check Cofinity-X regarding compliance with the provisions of this DPA, in particular the implementation of the technical and organizational measures; including by means of inspections.

4.12.3. Any inspections shall be subject to reasonable prior written notice and shall be conducted during normal business hours in a manner that minimises disruption to Cofinity-X's operations and protects Cofinity-X's trade and business secrets, as further set out in Sections 4.12.4 and 4.12.5. Cofinity-X shall cooperate with such inspections and shall not unreasonably withhold or delay its cooperation. At Cofinity-X's election, proof of compliance with the obligations under this DPA may alternatively be furnished by means of the mechanism described in Section 4.12.6, which the Customer shall accept as satisfying its audit rights under this DPA and under Article 28(3)(h) GDPR.

4.12.4. Cofinity-X shall be entitled, at its own discretion, considering the Customer's legal obligations, not to disclose information which is sensitive regarding Cofinity-X's business or if Cofinity-X would violate legal or other contractual regulations by disclosing it. The Customer shall not be entitled to have access to data or information on other clients of Cofinity-X, to information regarding costs, to quality review and contract management reports and to any other confidential or commercially sensitive data of Cofinity-X which is not directly relevant for the agreed review purposes.

4.12.5. If the Customer commissions a third party to carry out the inspection, the Customer shall oblige the third party in writing in the same way as the Customer is obliged to do based on this DPA. In addition, the Customer shall oblige the third party to maintain secrecy and confidentiality, unless the third party is subject to a professional confidentiality obligation. Upon request of Cofinity-X, the Customer shall immediately submit the obligation agreements with the third party to Cofinity-X. The Customer may not commission a competitor of Cofinity-X with the inspection.

4.12.6. At Cofinity-X's option, proof of compliance with the obligations under this DPA may also be provided by the submission of a suitable, up-to-date attestation or report by an independent body (e.g., auditor, audit, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit instead of by an inspection, if the audit report reasonably enables the Customer to satisfy itself of compliance with the contractual obligations.

5. Liability

The exclusions and limitations of liability under the Main Contract shall apply to Cofinity-X's liability under this DPA. Insofar as third parties assert claims against Cofinity-X which have their cause in a culpable breach by the Customer of this DPA or of one of its obligations as a controller, the Customer shall indemnify Cofinity-X against these claims upon first request.

Cofinity-X shall be entitled to disclose details of Cofinity-X's instructions and of the data processing carried out for the purpose of its own release from liability pursuant to Art. 82 para. 3 GDPR. The Customer shall take all necessary steps to ensure that Cofinity-X can indemnify itself against third parties in this context.

The Customer undertakes to indemnify Cofinity-X also against any fines imposed on Cofinity-X to the extent that the Customer bears a share of the responsibility for the violation sanctioned by the fine.

6. Final Provisions

If individual provisions of this Agreement are or become invalid or contain a loophole, this shall not affect the remaining provisions. The parties undertake to replace the invalid provision with a legally permissible provision that comes as close as possible to the purpose of the invalid provision and meets the requirements of Art. 28 of the GDPR.

If any provision of the Main Contract conflicts with this DPA, the DPA prevails to the extent of the conflict as it concerns the Processing of Customer Personal Data.

Annex 1

Details of Processing

A. LIST OF PARTIES

1. Data Exporter

Name: The party identified as the "Customer" in the Main Contract and this DPA
Address: _____ As set forth in the Main Contract
Contact person's name, position, and contact details: As set forth in the Main Contract
Activities relevant to the data transferred under this DPA: See Annex 1(B) below
Signature and date: This Annex I shall automatically be deemed executed when the Main Contract is executed by _____ Customer
Role: Controller or Processor

2. Data Importer

Name: As set forth in the Main Contract
Address: _____ As set forth in the Main Contract
Contact person's name, position, and contact details: Privacy Team of Cofinity-X, privacy@cofinity-x.com
Activities relevant to the data transferred under this DPA: See Annex 1(B) below
Signature and date: This Annex I shall automatically be deemed executed when the Main Contract is executed by _____ Cofinity-X
Role: Processor

B. DESCRIPTION OF PROCESSING

1. Nature and scope of data processing

Cofinity-X is the first operator of the Catena-X dataspace, enabling secure, sovereign, decentralized data exchange between participants in the automotive value chain. Cofinity-X provides the technical foundations for companies to exchange data securely while retaining full data sovereignty. In general, Cofinity-X does not store or access customer data in the provision of its services, but provides the infrastructure and marketplace through which participants exchange data in accordance with Catena-X standards. Although Cofinity-X focuses on business/industrial data, some personal data may be processed indirectly for operational purposes.

2. Types of personal data

The subject of processing of personal data are the following types/categories of data:

- Personal master data
- Communication data (e.g. telephone, e-mail)
- Contract master data (contractual relationship, address data, product or contractual interest)
- Contract billing and payment data

Categories of data subjects

The categories of data subjects affected by the processing include:

- Controllers
- Controllers' selected Employees

Annex 2

Technical and organizational measures

1. Overview and Responsibility Model

Cofinity-X implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in accordance with Art. 32 GDPR.

The services are operated on cloud infrastructure provided by recognized professional Cloud Service Providers (such as Azure or Amazon Web Services) under a shared responsibility model:

- Cloud Service Providers are responsible for physical data-center security, infrastructure resilience, and environmental protections.
- Cofinity-X is responsible for logical security, access control, application security, and organizational safeguards.

Compliance of cloud infrastructure is evidenced by recognized certifications such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2, and equivalent assurance reports.

2. Confidentiality

2.1 Physical Security

Personal data is processed exclusively in professionally operated cloud data centers with robust physical security controls, including:

- Perimeter protection, access-controlled entrances, and monitored security zones
- Video surveillance, intrusion detection, and alarm systems
- Visitor management, logging, and supervised access
- Role-based physical access and separation of secure areas

These measures are fully implemented and operated by the cloud providers and regularly audited via independent certifications.

2.1.1 Office and Workplace Security

Cofinity-X maintains access-controlled office environments.

- Access to office premises is restricted to authorized personnel and managed visitors and follows defined visitor management procedures.
- Processing systems containing personal data are not operated in publicly accessible areas.
- Physical access to offices does not permit direct access to cloud infrastructure or production environments.

2.2 Logical Access Control

Unauthorized system access is prevented through:

- Strong authentication mechanisms, including multi-factor authentication (MFA)
- Role-based and function-based authorization concepts
- Principle of least privilege and need-to-know
- Regular review and adjustment of access rights
- Secure password policies and encrypted credential storage
- Network segmentation and firewall protection
- Secure endpoint and mobile device management

2.3 Data Access and Processing Control

Access to personal data is restricted so that unauthorized reading, modification, copying, or deletion is prevented:

- Clearly defined administrative roles with minimized privileges
- Separation of duties and four-eyes principle for critical operations
- User-specific access logging and monitoring
- Controlled and documented deletion processes
- Secure destruction of data carriers and documents in accordance with recognized standards
- Defined policies for remote work and home office scenarios

2.4 Separation of Data

Data processed for different purposes or customers is logically separated through:

- Tenant-based logical isolation
- Database and authorization-level separation
- Separation of production, test, and development environments
- Purpose-bound access restrictions

Where appropriate, pseudonymization or anonymization is applied in accordance with processing purpose and risk.

3. Integrity

3.1 Secure Data Transmission

Integrity and confidentiality during transmission are ensured through:

- Encryption of data in transit using state-of-the-art cryptographic methods
- Secure file exchange and collaboration platforms
- Encrypted mobile devices and portable media
- Binding confidentiality obligations for all personnel

3.2 Input and Change Control

Cofinity-X ensures traceability of data processing through:

- Logging of data entry, modification, and deletion
- Role-based write permissions
- User-specific action traceability
- Controlled document and change management processes
- Clearly assigned responsibilities for data modifications and deletions

4. Availability and Resilience

4.1 Availability

Availability of personal data is protected through:

- Highly available cloud infrastructure
- Encrypted backups with defined retention periods
- Continuous monitoring of system availability and performance
- Regular patching and vulnerability management
- Malware and threat protection measures
- Incident and emergency communication procedures

Physical resilience measures (e.g. power supply, fire protection, environmental monitoring) are fully provided by the cloud providers.

4.2 Recoverability

Measures exist to restore availability and access to personal data in the event of an incident:

- Documented emergency and recovery concepts
- Backup and restore procedures
- Regular testing of recovery capabilities aligned with contractual requirements

5. Organizational Measures and Continuous Improvement

Cofinity-X maintains comprehensive organizational controls, including:

- Information Security Management System
- Data protection Management System
- Appointment of a Data Protection Officer
- Designation of a Chief Information Security Officer
- Regular data protection and security training for employees
- Procedures for handling data subject rights and personal data incidents
- Privacy-by-design and privacy-by-default principles
- Contractual control of subprocessors pursuant to Art. 28 GDPR
- Regular review, assessment, and evaluation of TOM effectiveness

6. Compliance Evidence

The effectiveness of these measures is demonstrated through:

- Recognized cloud provider certifications and audit reports
- Internal policies, procedures, and training records
- Logging, monitoring, and incident documentation

Annex 3

List of Subprocessors

For Customer Personal Data processing on behalf of the Customer, Cofinity-X may use the services of third parties who process data on its behalf ("Subprocessors").

Company	Address	Scope of data processing	Place of data processing
Hubspot, Inc.	25 First Street, 2nd floor, Cambridge, MA 02141, USA.	Customer relationship management and newsletter delivery.	Mainly Europe. Subprocessor may process data in the United States. Subprocessor is certified under the EU-US Data Privacy Framework and is therefore covered by the European Commission's adequacy decision for the United States.
Sendgrid (Twilio, Inc.)	101 Spear Street, 5th Floor San Francisco, CA 94105, USA	Customer communication.	Mainly Europe. Subprocessor may process data in the United States. Subprocessor is certified under the EU-US Data Privacy Framework and is therefore covered by the European Commission's adequacy decision for the United States.
Nordcloud	Mies-van-der-Rohe-Straße 6 80807 München, Germany	Cloud-native implementation, application development, and managed services.	Mainly Europe. Subprocessor may process data in the United States. Subprocessor is certified under the EU-US Data Privacy Framework and is therefore covered by the European Commission's adequacy decision for the United States.
Jira (Atlassian, Inc.)	350 Bush Street, Level 13, San Francisco, California 94104, USA.	Ticket system to respond to support requests.	Mainly Europe. Subprocessor may process data in the United States. Subprocessor is certified under the EU-US Data Privacy Framework and is therefore covered by the European Commission's adequacy decision for the United States.
AWS	Marcel-Breuer-Straße 12, 80807 München	Cloud Service Provider.	Mainly Europe. Subprocessor may process data in the United States. Subprocessor is certified under the EU-US Data Privacy Framework and is therefore covered by the European Commission's adequacy decision for the United States.

Azure	Dublin 18, D18 P521, Ireland	Cloud Service Provider.	Mainly Europe. Subprocessor may process data in the United States. Subprocessor is certified under the EU-US Data Privacy Framework and is therefore covered by the European Commission's adequacy decision for the United States.
M365	Burchardstraße 14, 20095 Hamburg	Cloud-based collaboration and documentation services.	Mainly Europe. Subprocessor may process data in the United States. Subprocessor is certified under the EU-US Data Privacy Framework and is therefore covered by the European Commission's adequacy decision for the United States.
Intercom, Inc.	55 2nd Street, 4th Floor, San Francisco, CA 94105, USA	Messaging and communication on our website, including an AI chatbot.	Mainly Europe. Subprocessor may process data in the United States. Subprocessor is certified under the EU-US Data Privacy Framework and is therefore covered by the European Commission's adequacy decision for the United States.