Wandelbots Data Processing Agreement

by and between

Customer as defined in the Wandelbots General Terms and Conditions and underlying order

- Controller -

and

Wandelbots GmbH, with business seat in Dresden/Germany

- Processor -

about a commissioned processing in the sense of Art. 28 para. (3) of the General Data Protection Regulation (GDPR).

Preamble

This Data Processing Agreement outlines the obligations of the parties regarding data protection resulting from the processing described in detail in the Wandelbots General Terms and Conditions and the underlying accepted offers/order(s) or individual agreements (“Agreement”).

The terms of this Data Processing Agreement shall apply to all activities related to the Agreement in which employees of the Processor or third parties engaged by the Processor process personal data ("Data") on behalf of the Controller.

If not specifically set out otherwise in this Data Processing Agreement, the definitions from the Agreement shall also apply to this Data Processing Agreement.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 5

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 6

Obligations of the Parties

6.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

6.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

6.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

6.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

6.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

6.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least two weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a subprocessor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the subprocessor contract and to instruct the sub-processor to erase or return the personal data.

6.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 6.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the subprocessor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 7

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 8

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

8.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

8.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 9

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 6.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

LIST OF PARTIES

Controller:

Customer as defined in the Wandelbots General Terms and Conditions and underlying order/offer/individual agreement

Processor:

Name: Wandelbots GmbH

Address: Tharandter Straße 33, 01159 Dresden, Germany

Contact person's name, position and contact details: Richard Bode, DPO, datenschutz@wandelbots.com

ANNEX II:

DESCRIPTION OF THE PROCESSING

Subject matter

Provision of the services agreed between the parties.

Nature of the processing

Automated and manual processing of personal data within Wandelbots' systems, including storage, access, use, transmission and deletion, as necessary to provide the services

Purpose of the processing

Fulfilment of the services as specified in the Wandelbots General Terms and Conditions and the underlying order(s)/offer(s) or individual agreements.

Duration of processing

Duration of the services agreed between the parties.

Categories of personal data

- Contact data
- Software usage data
- Additional data provided by the controller

Categories of data subjects

- Employees of the controller
- Customers of the controller

Special categories of personal data (sensitive data)

No special categories of personal data are required for the provision of services.

ANNEX III

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Pursuant to Article 32 GDPR, Wandelbots is legally obliged to implement technical and organizational measures (TOMs). The overall goal is to ensure a level of security appropriate to the data protection risk which inherently follows from the processing of personal data. As follows from the name, TOMs can be of a technical- and organizational nature. Below is an overview of the TOMs with a description of each measure.

TOM	Description
2FA implementation	Two-factor authentication (2FA), which combines two independent factors, e.g. password and authenticator app.
Access control for the use of a data processing system	Measures to ensure that those authorized to use a data processing system can access only the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage have been implemented. These include: • Authorization concept • Administration of rights by system administrator • Number of administrators reduced to the "bare minimum" • Password policy incl. Password length, password change • Logging of changes to and deletion of data | Secure storage of data media • Physical deletion of data media before reuse • Proper destruction of data media (DIN 32757) • Encryption of data media.
Authorization procedure for information processing equipment	A formal approval procedure is implemented, which systems and applications with personal data have to go through before they are allowed network access. Cf. ISO 27001, Annex A.6.1.4 "Approval procedure for information processing facilities".
Bring Your Own Device (BYOD)	The use of private hardware or end devices (Bring Your Own Device - BYOD) may not be used for the processing of personal data, and only connected to the guest Wi-Fi.
Clean desktop- and locking policy	Employees are obligated to ensure no sensitive and/or confidential documentation remains on their desk, clearly visible for anyone to see, and to lock the device when leaving the workplace.
Continuous updating of the data protection management system (DPMS)	At a yearly interval, the data protection management system is checked for topicality and adapted to new events (e.g. new processes, new software), and documented.

Contract management system	Appropriate measures regarding access authorizations, compliance requirements, decision-making powers, deadline controlling, contract filing and transparency in the context of steering (stakeholders), are implemented.
Data classification	There is a company-wide valid scheme for the classification of data. Cf. ISO 27001, Annex A.7.2.1 "Rules for classification". The company-wide procedure for handling classified data is implemented in practice. Cf. ISO 27001, Annex A.7.2.2 "Identification and handling of information".
Document management with versioning system	Documents to be archived are stored in a document management system with a versioning option for the documents.
Documentation of the Data Protection Management System (DSMS).	The data protection management system is documented with all legally relevant aspects, and is designed and administered by the relevant persons in the data protection organization.
Documentation of the existing IT infrastructure and protection requirements	The assets (IT components in need of protection) are systematically documented. It is clear which processes and which data are processed by these components. The need for protection is derived from the criticality of the processes and the data processed (e.g. special personal data or trade secrets).
Email security (encryption, sandboxing)	Emails are encrypted in transit, and there is a protection layer for e-mail security by scanning files for malware separately from the system environment.
Emergency plan for IT operating problems implemented	There is a process for escalating IT problems. In this process it is defined to whom and what form problems discovered are to be reported. Problems are to be classified according to severity. Depending on the severity of the problem, the decision level at which the problem is to escalate is determined.
Encryption of databases	Database systems used to process personal data keep the data encrypted. The data flow between application and database is encrypted (TLS).
Establishment of data protection organization	The data protection organization is documented with the associated persons and roles. The privacy organization sets privacy goals, handles privacy issues, and develops the privacy management system, and is chaired by the Data Protection Officer.
Full disk encryption for PCs and notebooks (hardware-based encryption)	State-of-the-art measures for hard disk encryption are implemented on each client. Full hard disk encryption is set up on PCs and notebooks and cannot be deactivated by the user. Recovery keys are stored securely. An access concept for managing the keys exists. Hard disk encryption is only used in conjunction with a complete, regular and monitored system backup. Workarounds exist in the event of errors to maintain operational capability.
Home office / teleworking: Appropriate design of the workspace	The workstation is selected in such a way that family members or visitors cannot look at the notebook or paper documents (no access to personal data by third parties). Corresponding regulations are implemented.

Identity Management (IM) and Identity and Access Management (IAM)	Measures for organizing the assignment of rights and roles within information technology (IT): Identity Management (IM) for the audit-proof assignment of authorizations for IT processes and applications in companies and organizations. Process for creating user IDs, approving and revoking access authorizations, and access management for web portals, processes, and services, single sign-on (SSO) as part of a one-time authentication or security policy.
Implementation of data protection-friendly default settings (privacy by default)	Data protection-friendly default settings are taken into account in product development.
Information security management (IT security, ISMS), information security and data security	Implementation of technical, organizational and personnel security measures (ISMS) to minimize risks and improve information and IT security (IT security and data protection, KRITIS risks) based on the requirements of known standards (BSI basic protection, ISO27001) and to secure critical infrastructures for KRITIS operators.
IT Landscape documentation	The company's own system landscape is documented, and network plans exist. There is a complete overview of all IT assets (all hardware and software). The complete functions of all components used in the network are known and configured in a data protection-friendly manner (privacy by default). Foreign, harmful or unauthorized components can be identified. Updating of asset management is defined and takes place at regular intervals. Employees are prohibited from removing, relocating or adding components of the IT equipment on their own authority. Only the IT administrators have administrative rights to install and commission new components. The IT documentation contains at least structured information on the following topics: • Systems and applications used and the dependency of business processes on these systems. • Physical and logical network structure and security zones • Analysis of tolerable downtime for critical systems and/or applications. • Provision of redundancies or reserve systems. • Measures for restoring functionality after system failure in the defined time window • Backup concept, backup checks, technologies used, recovery and restart plans. • Firewall systems, zone definitions, firewall rules, VPN accesses. • Maintenance and update concept for software and hardware used.

	• Access and rights concept according to group guidelines.
IT security in the home office (data protection guideline for home office/teleworking)	Appropriate measures (cyber security precautions) are taken and implemented to increase cyber security. These include clear regulations for working from home and the disclosure of contact persons in the event of queries.
IT security incident management	Identification and consistent documentation of security incidents (reporting channel, security reporting) as well as regular training and awareness-raising measures to increase security awareness in order to reduce the damage caused by cybersecurity attacks.
Information security management	A suitable organizational structure for information security has been established. Information security is integrated into the organization-wide processes and procedures. In addition to the IT manager, the data protection officer (DPO) is also involved in the process of implementing security requirements.
Logging of Internet access (data security)	Determining whether intrusion attempts have been made into the network through the Internet, and whether connection data has been collected as part of unlawful Internet use.Logging of Internet accesses to determine the cost of resources consumed (expenses). Ensuring data protection principles (data economy, purpose limitation, anonymization, deletion periods, security against manipulation) for collecting log data in compliance with data protection regulations.
Logging the activities of the system administrators	System events, data accesses, etc. are documented in the company, to detect gaps, misuse and external attacks more quickly, and in order to prevent data loss and damage to the company's image.
Loss and theft of mobile devices	The loss or theft must be reported immediately to the manager. In the context of mobile device management, the information reaches the IT department. There, the immediate deletion and search of the device is started. In case of theft, the management files a report immediately. The process is documented in Jira with indication of the diary number or, in the case of loss, with indication of the course of the loss in the activity manager. The following IT components count as mobile end devices in the company: • notebooks • tablets • smartphones / mobile phones.
Mobile Device Management	A mobile device management system is in use. Care was taken to ensure that data protection-friendly default settings ensure that people (employees) cannot be controlled or monitored, but that the focus of the deployment is exclusively on IT security.

Network security	The internal network is protected by a firewall, which as a minimum requirement enables data flow control in the incoming and outgoing direction. The application of software updates/patches is rule-based and fully automated.
Off-Boarding process in place	There is a sufficient off-boarding process in place to deal with people leaving the company. All accesses are blocked. The business documents created by the departing person and the business e-mails (inbox and outbox) are secured or their further use is regulated.
Password policy	Internal guidelines for password creation and use are defined and communicated (Data and IT Security Policy). Rules for blocking and reassigning passwords after an incident. Default settings resulting from the configuration options of the operating system used (policy) have been set up. The criteria specified by the recommendations of state security authorities have been taken into account. In addition, the default passwords preset on the network components have been changed as a minimum measure to prevent unauthorized persons from re-configuring the network components. This ensures that only authorized persons have logical access to the network components.
Physical security of premises	Physical access control limits access to sites, offices or rooms. The company has regulations, processes and technical requirements to ensure access control. Moreover, alarm systems are in place, as well as video surveillance.
Reporting system for technical malfunctions	There is an established ticket system (Jira) for communication with the IT department. This ticket system is used to report outages, incidents, problems, etc., which are also logged there on a long-term basis.
Software / Supplier approval procedure	Selection criteria according to customer requirements for products and services for supplier selection according to ISO 9001, are implemented. Software and programs are obtained exclusively from trustworthy sources to ensure the integrity and functionality of the software. As part of the general security measures, attention is also paid to any hidden software components (toolbars, adware, etc.).
Signing documents electronically	A procedure has been implemented with which documents can be signed electronically via DocuSign.
Use of VPN network	State-of-the-art VPN mechanisms are used for external access (e.g., home office workstations or mobile access) to internal company systems. The set of rules for VPN access through the firewall is coordinated and documented with the person responsible for the system and limited to the systems, ports and protocols required for the function.
Visitor management	There is a process for welcoming strangers or visitors or guests, escorting them to their destination and tracking their whereabouts on the organization's premises. Non-company personnel cannot move around the premises

	independently and are issued a visitor badge which they wear visibly during the visit.
Wired access: network admission control	It is ensured that only authorized devices have logical access to the organization's network. Cf. ISO 27001, Annex A.11.4.3.

ANNEX IV:

LIST OF SUB-PROCESSORS

Name and address	Contact person's name, position and contact details	Description of the processing	Third country in case of international data transfer, and transfer instrument where applicable	Optional (Y/N)
Atlassian. Pty Ltd. c/o Atlassian 350 Bush St, Floor 13 San Francisco, CA 94104 USA	Privacy Team eudatarep@atlassian.com	Ticketing and documentation of support requests	Data are processed in the European Union (EU) and the USA, Standard Contractual Clauses, Article 46(2)(c) GDPR	N
Cryptlex LLP 16192 Coastal Highway Lewes, DE 19958, USA	Privacy & Security Team security@cryptlex.com	License management	Data are processed in the European Union (EU) and the USA, Standard Contractual Clauses, Article 46(2)(c) GDPR	N
HYCU Ltd. 10 Earlsfort Terrace, Dublin 2, D02 T380 Ireland	Privacy Team privacy@hycu.com	Backup management	Data are processed in the European Union (EU).	N

Microsoft Ireland Operations Ltd One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Privacy Team https://aka.ms/privacyresponse	Hosting, communication for support requests	Data are processed in the European Union (EU) and the USA, Standard Contractual Clauses, Article 46(2)(c) GDPR	N
Okta, Inc. 100 First Street, San Francisco, CA 94105 USA	Privacy Team privacy@okta.com	Authentication	Data are processed in the European Union (EU) and the United States of America, Standard Contractual Clauses, Article 46(2)(c) GDPR	N
Slack Technologies Limited Salesforce Tower 60 R801, North Dock Dublin, Ireland	Privacy Team privacy@slack.com	Communication for support requests	Data are processed in the European Union (EU) and the USA Standard Contractual Clauses, Article 46(2)(c) GDPR	Y