

HARDWARIO CLOUD

HARDWARIO Cloud Data Processing Agreement

How HARDWARIO a.s. processes personal data on behalf of its customers in HARDWARIO Cloud, under Article 28 of the General Data Protection Regulation.

DOCUMENT: HLN.261009.03-R1 VALID FROM: October 9, 2026

CONTENTS

1. Parties and scope	1
2. Roles	2
3. Instructions	2
4. Confidentiality	2
5. Security	3
6. Sub-processors	3
7. Data subject rights	3
8. Assistance and personal data breaches	3
9. Return and deletion	4
10. Information and audits	4
11. Transfers outside the European Economic Area	4
12. Liability and final provisions	4
Annex I: Description of the processing	5
Annex II: Technical and organisational measures	5
Annex III: Sub-processors	6

1. Parties and scope

1.1. Parties. This Data Processing Agreement (the "DPA") is concluded between the customer of HARDWARIO Cloud (the "Customer", controller) and HARDWARIO a.s. (the "Processor"):

Company	HARDWARIO a.s.
Company ID	04998511
VAT ID	CZ04998511
Registered office	U Jezů 525/4, 460 01 Liberec, Czech Republic
Register entry	Commercial Register kept by the Regional Court in Ústí nad Labem, Section B, Insert 2864
Contact	ask@hardwario.com, www.hardwario.com

1.2. Scope. The DPA applies whenever the Processor processes personal data on the Customer's behalf in providing HARDWARIO Cloud and the related support (the "Service"), whether the Customer contracted under the HARDWARIO Cloud Terms of Service HLN.261009.02 (the "Terms"), under an individual contract, or

through a HARDWARIO partner. It forms part of that contract (the "Principal Agreement") and is concluded together with it.

1.3. Partners. A HARDWARIO partner through which the Customer bought the Service is not a party to this DPA. A partner that itself accesses the Customer's personal data (for example in first-line support) does so as the Customer's separate processor under its own agreement with the Customer.

1.4. Definitions. "GDPR" means Regulation (EU) 2016/679. "Personal Data" means the personal data the Processor processes on the Customer's behalf, as described in Annex I. "Sub-processor" means a third party the Processor engages to process Personal Data. "SCCs" means the standard contractual clauses under Commission Implementing Decision (EU) 2021/914. Other terms ("controller", "processor", "processing", "personal data breach") have the meaning given in the GDPR.

2. Roles

2.1. The Customer is the controller and the Processor the processor of the Personal Data. Where the Customer itself acts as a processor for another controller, the Customer confirms it is authorised to give the instructions in this DPA, and the Processor acts as a sub-processor.

2.2. The Processor is a separate controller, not a processor, of the data it needs to run its own business: the sign-in data of user accounts, contract, billing and support communication with the Customer, and the operational and security logs of the Service. That processing is described in the HARDWARIO Privacy Notice, published at <https://www.hardwario.com/legal/>.

2.3. In matters of personal data this DPA prevails over the Principal Agreement.

3. Instructions

3.1. The Processor processes Personal Data only on the Customer's documented instructions, including with regard to transfers to third countries, unless European Union or Member State law requires otherwise; in that case it informs the Customer before processing, unless that law prohibits it on important grounds of public interest.

3.2. The Customer's documented instructions are the Principal Agreement, this DPA and the Customer's use and settings of the Service. Further instructions require agreement and may be subject to a fee.

3.3. The Processor informs the Customer without delay if, in its opinion, an instruction infringes data protection law, and may suspend the affected processing until the instruction is confirmed or changed.

3.4. The Customer is responsible for the lawfulness of the processing: it has a legal basis, informs the data subjects and, where it relies on consent, obtains it. The Customer does not submit special categories of personal data, data on criminal convictions or data of children to the Service unless agreed in writing.

4. Confidentiality

The Processor ensures that the persons authorised to process Personal Data are bound by confidentiality, contractual or statutory, that continues after their engagement ends, and gives them access only to the extent needed to provide, secure and support the Service.

5. Security

5.1. The Processor takes appropriate technical and organisational measures under Article 32 GDPR, taking into account the state of the art, the costs and the nature, scope, context and purposes of the processing and the risks to data subjects. The measures in force are described in Annex II.

5.2. The Processor may change the measures if the overall level of protection is not reduced.

5.3. The Customer is responsible for its settings of the Service: the users it invites and their roles, the API keys it creates, its connectors and their endpoints, and the security of its devices and of its own systems.

6. Sub-processors

6.1. General authorisation. The Customer gives the Processor general written authorisation to engage Sub-processors. The Sub-processors at the date of this DPA are listed in Annex III; the current list is published at <https://www.hardwario.com/legal/cloud-data/>.

6.2. Changes. The Processor informs the Customer of an intended addition or replacement of a Sub-processor by e-mail to the account owner at least 30 days in advance, and updates the published list.

6.3. Objection. The Customer may object to the change on reasonable grounds of data protection within those 30 days. If the parties do not resolve the objection, the Customer may terminate the Principal Agreement with effect before the change applies, without any charge for termination.

6.4. Obligations. The Processor imposes on each Sub-processor by contract the same data protection obligations as in this DPA, in particular sufficient guarantees of appropriate technical and organisational measures, and remains fully liable to the Customer for the Sub-processor's performance.

7. Data subject rights

7.1. Taking into account the nature of the processing, the Processor assists the Customer by appropriate technical and organisational measures in responding to requests of data subjects exercising their rights under Chapter III GDPR. The Customer first uses the functions of the Service (viewing, editing, exporting and deleting data, managing users).

7.2. If a data subject contacts the Processor directly about Personal Data, the Processor refers them to the Customer and informs the Customer without delay; it does not answer the request itself unless the Customer instructs it to.

8. Assistance and personal data breaches

8.1. Assistance. Taking into account the nature of the processing and the information available to it, the Processor assists the Customer in meeting its obligations under Articles 32 to 36 GDPR: security, notification of breaches, data protection impact assessments and prior consultation. It may do so by providing documentation of the Service and of its measures.

8.2. Breach notification. The Processor notifies the Customer of a personal data breach affecting Personal Data without undue delay, and in any event within 48 hours of becoming aware of it, by e-mail to the account owner.

8.3. Content. The notification describes, as far as known and supplemented as information becomes available, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point.

8.4. The Processor does not notify the supervisory authority or data subjects on the Customer's behalf unless the Customer instructs it to or the law requires it. A notification is not an admission of fault.

9. Return and deletion

9.1. At the end of the Principal Agreement the Customer retrieves its data during the retrieval period under the Terms (clause 6.4) or the individual contract.

9.2. After the retrieval period the Processor deletes the Personal Data within 30 days; backups are overwritten within their 4-week cycle, and until then the Personal Data in them remains subject to this DPA. The Processor confirms the deletion in writing at the Customer's request.

9.3. The Processor keeps Personal Data after that only where European Union or Member State law requires it, and only for that purpose.

10. Information and audits

10.1. The Processor makes available to the Customer all information necessary to demonstrate compliance with Article 28 GDPR, in the first place in writing, for example by answering the Customer's security questionnaire.

10.2. Where the information does not suffice, the Customer may carry out an audit, including an inspection, itself or through an auditor bound by confidentiality who is not a competitor of the Processor, on 30 days' written notice, at most once in 12 months (more often after a personal data breach or at the request of a supervisory authority), during business hours and without risk to the data of other customers.

10.3. The Customer bears the costs of the audit, unless it reveals a material breach of this DPA by the Processor.

11. Transfers outside the European Economic Area

11.1. The Processor stores Personal Data in the European Union. It transfers Personal Data to a country outside the European Economic Area only in accordance with Chapter V GDPR: to a country or a recipient covered by an adequacy decision of the European Commission (including the EU-U.S. Data Privacy Framework), or under the SCCs or binding corporate rules. Annex III states the mechanism for each Sub-processor.

11.2. Where the Customer is established outside the European Economic Area, the transfer of Personal Data from the Processor to the Customer is governed, where required, by Module Four (processor to controller) of the SCCs, which are incorporated into this DPA by reference.

12. Liability and final provisions

12.1. The liability of the parties under this DPA is subject to the limitations of the Principal Agreement, except where data protection law does not allow them; the liability towards data subjects is not limited.

12.2. This DPA applies for as long as the Processor processes Personal Data on the Customer's behalf.

12.3. The Processor may change this DPA in the same way as the Terms (clause 14 of the Terms), in particular to reflect changes in the law or in transfer mechanisms. Each version carries a document number, revision and valid-from date, and all earlier versions remain available at <https://www.hardwario.com/legal/>.

12.4. This DPA is governed by Czech law; disputes are decided by the courts having jurisdiction at the Processor's registered office.

Annex I: Description of the processing

ITEM	DESCRIPTION
Controller	The Customer, as identified in its account or contract.
Processor	HARDWARIO a.s., ask@hardwario.com. The Processor has not appointed a data protection officer.
Subject matter and duration	Providing HARDWARIO Cloud and the related support for the term of the Principal Agreement, the retrieval period and the deletion period under clause 9.
Nature and purpose	Receiving, storing, organising, displaying, forwarding (connectors and the API), backing up and deleting data, and support at the Customer's request, in order to provide the Service.
Categories of data subjects	The Customer's users of the Service; persons to whom the data of the Customer's devices relates, for example employees using vehicles or rooms equipped with the devices; other persons whose data the Customer enters into the Service.
Categories of personal data	Names, e-mail addresses and roles of users; device data that can be linked to a person, such as location, measured values and timestamps; device identifiers and network data, including IP addresses; data the Customer enters in names, comments, tags and variables.
Special categories	None, unless agreed in writing.
Frequency	Continuous.
Retention	Device messages 12 months, unless the order or contract states a different period; other data for the term of the Principal Agreement; backups 4 weeks.
Supervisory authority	The authority of the Member State where the Customer is established; for the Processor, the Office for Personal Data Protection (Úřad pro ochranu osobních údajů), Prague, Czech Republic.

Annex II: Technical and organisational measures

The Processor's measures in force at the date of this DPA:

AREA	MEASURE
Location	The Service and its backups run in the data centre of DigitalOcean, LLC in Frankfurt am Main, Germany.
Encryption in transit	The web interface, the API and the connectors (webhooks) communicate over TLS (HTTPS).
Device communication	Device messages are authenticated with a message authentication code. Devices based on the nRF9151 encrypt their communication with DTLS. Devices with HARDWARIO SIM cards connect through a private APN of Vodafone Czech Republic and an IPsec tunnel (IKEv2, AES-256, SHA-256, MODP-2048 group) to the Service.

AREA	MEASURE
Separation	Each customer's devices, data and users are kept in separate Spaces; a user sees only the Spaces to which they were invited.
Access control	Users sign in with a password and a verified e-mail address, or with a Google or Microsoft account. Within a Space, access follows the roles owner, administrator (full access) and user (read only). Programmatic access uses API keys that the Customer creates and revokes.
Backups	The Service is backed up weekly; each backup is kept for 4 weeks.
Vulnerability handling	Vulnerabilities are reported to security@hardwario.com and handled under the Coordinated Vulnerability Disclosure Policy HLN.261009.01 and the internal procedure HCP.261009.01, including reports under Regulation (EU) 2024/2847.
Confidentiality of staff	Persons with access to Personal Data are bound by confidentiality (clause 4).

Annex III: Sub-processors

SUB-PROCESSOR	ACTIVITY	LOCATION	TRANSFER MECHANISM
DigitalOcean, LLC	Hosting, storage and backups of the Service	Frankfurt am Main, Germany	Data stored in the EU; EU-U.S. Data Privacy Framework
Twilio Inc. (SendGrid)	Sending e-mails from the Service (invitations, notifications)	USA	Binding corporate rules
Vodafone Czech Republic a.s.	Mobile connectivity of devices with HARDWARIO SIM cards (private APN)	Czech Republic	Not applicable (EU)
Google Ireland Limited, Google LLC	E-mail for support communication (Google Workspace)	EU, USA	EU-U.S. Data Privacy Framework

Signing in with a Google or Microsoft account is a service of Google and Microsoft, which act as separate controllers, not as Sub-processors.