HOSTZONE s.r.o.

Data processing agreement

Effective from: 1 September 2026

Last updated: 1 September 2026

Version: 2026-09-01

HOSTZONE s.r.o., IČO 248 81 465, DIČ CZ24881465
Příčná 1892/4, Nové Město, 110 00 Praha 1, Czech Republic
Obchodní rejstřík: C 443830
support@hostzone.eu · +420 2 1001 4678
https://hostzone.eu/en/legal/data-processing/

Article 1 - The parties and the relationship to the Terms

1.1 The **Processor** is HOSTZONE s.r.o., company no. 248 81 465, registered office at Příčná 1892/4, Nové Město, 110 00 Prague 1, Czech Republic, entered in the commercial register kept by the Municipal Court in Prague, file no. C 443830.

1.2 The **Controller** is the Customer who has concluded a Contract with the Processor under the Terms.

1.3 This agreement (the "**DPA**") governs the processing of personal data under Article 28 GDPR that occurs in providing the Services under the Terms. Where they conflict, the DPA prevails over the Terms in matters of personal data protection.

1.4 Terms not defined here have the meaning given in the Terms or in the GDPR.

Article 2 - The parties' roles

2.1 The Customer is the **controller** of the personal data it stores, makes available or otherwise processes through the Service (the Content under Article 2.7 of the Terms). In relation to that data the Processor is a **processor**.

2.2 The Customer is responsible for having a legal basis for the processing, for having met its information duty towards data subjects, and for being entitled to engage the Processor to carry out the processing.

2.3 In relation to data the Processor processes for **its own** purposes - in particular the Customer's identification and billing data, operational and security logs, and correspondence with support - the Processor is a **separate controller**. The DPA does not govern that data; it is governed by the Privacy policy.

Article 3 - Subject matter, nature, purpose and duration of the processing

3.1 **Subject matter:** providing hosting and related services under the Contract.

3.2 **Nature and purpose:** storing, making available, transmitting and backing up the Content to the extent necessary to run the Service. The Processor does not access the Content except in the cases under Article 5.2.

3.3 **Duration:** for the term of the Contract and thereafter for the period under Article 12.

3.4 The categories of data subjects and the types of personal data are set out in **Annex 1**.

Article 4 - The controller’s instructions

4.1 The Processor processes personal data **solely on the Customer’s documented instructions**. The Contract itself, the Terms and this DPA are treated as such an instruction.

4.2 An act the Customer performs in the Customer Portal, in cPanel or in its own application is also treated as a documented instruction.

4.3 The Processor will process data beyond the instructions only where required to do so by EU or Member State law. In that case it will inform the Customer beforehand, unless that law prohibits it on important grounds of public interest.

4.4 The Processor will inform the Customer if it considers that an instruction infringes the GDPR or other data protection legislation. It is under no duty to review instructions in law.

Article 5 - Access to the Content

5.1 The Processor does not access or inspect the Content systematically.

5.2 Access is permissible only:

- at the Customer’s express request, normally when handling a support request,
- where necessary to remedy a fault or to restore the Service,
- on reasonable suspicion of a breach of the AUP or of a threat to security,
- where required by a legal obligation or a decision of a public authority.

5.3 The Processor keeps a record of access under the second to fourth indents.

Article 6 - Confidentiality

6.1 The Processor ensures that persons authorised to process personal data are bound by **confidentiality** or are under a statutory duty of confidentiality. The obligation continues after the co-operation ends.

6.2 Access to the systems is held by the operator and by authorised collaborating persons acting on the Processor’s instructions.

6.3 The Processor limits access to persons who need it to carry out their tasks, and to the extent sufficient for that.

Article 7 - Security

7.1 The Processor has put in place technical and organisational measures under Article 32 GDPR, described in **Annex 2**.

7.2 The Processor may change the measures provided it does not thereby reduce the level of security achieved. The current wording of Annex 2 is available on the Processor’s website.

7.3 The Customer acknowledges that **securing its own application, its updates, passwords and credentials is a matter for the Customer**. The Processor is not liable for vulnerabilities in the Content or in applications the Customer runs.

Article 8 - Sub-processors

8.1 The Customer gives the Processor **general authorisation** to engage further processors. The current list is published on a separate page, Sub-processors.

8.2 The Processor operates the Services **on its own servers housed in a data centre within the European Union**. The storage media are **encrypted**. The data centre operator provides only physical space, power, connectivity and physical security and has no logical access to the data.

8.3 The Processor imposes on every sub-processor **the same obligations** in data protection as it has itself under the DPA, and **is liable for their performance** as for its own.

8.4 **Optional third-party services.** Within LiteSpeed Enterprise the Customer may activate the QUIC.cloud CDN. Activation is the Customer's own act; if the Customer performs it, it is **the Customer** who brings the CDN provider into the processing and who is responsible for the legal basis and for its own contractual relationship with that provider. Without activation no traffic is routed through the CDN.

8.5 The Processor informs the Customer of an intended **change** to the list of sub-processors at least **30 days in advance** by e-mail or in the Customer Portal.

8.6 Within 30 days the Customer may raise a **reasoned objection** to the change. If no agreement is reached, the Customer may terminate the Contract to the extent concerned as at the day the new sub-processor is engaged, with a refund of the pro-rata part of the price paid.

Article 9 - Assistance with data subjects' rights

9.1 The Processor gives the Customer **reasonable assistance** in handling data subjects' requests under Chapter III GDPR, by appropriate technical and organisational measures.

9.2 If a data subject approaches the Processor directly with a request, the Processor **does not handle it** and passes it to the Customer without undue delay.

9.3 The Customer has full access to the Content and will handle most requests itself. Where assistance beyond ordinary administration calls for disproportionate effort, the Processor may charge for it according to the time actually spent.

Article 10 - Assistance under Articles 32 to 36 GDPR

10.1 The Processor gives the Customer assistance in ensuring compliance with Articles 32 to 36 GDPR, taking into account the nature of the processing and **the information available to it**.

10.2 Assistance with a data protection impact assessment (DPIA) and with prior consultation is limited to providing the description of the measures under Annex 2 and information about the infrastructure.

Article 11 - Personal data breaches

11.1 Where the Processor discovers a breach of the security of personal data processed for the Customer, it will notify the Customer **without undue delay**, and at the latest within **48 hours** of discovery.

11.2 The notification contains, where possible: a description of the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken and proposed, and a contact point.

11.3 Where not all the information is available at once, the Processor will provide it in stages without undue delay.

11.4 **Notification to the supervisory authority and to data subjects is made by the Customer** as controller. The Processor will assist it in doing so.

Article 12 - The fate of the data after the end

12.1 After the Contract ends the Processor will, at the Customer's choice, **delete or return** the personal data and delete existing copies, unless required to retain them under EU or Member State law.

12.2 Return under Article 12.1 is effected **by making the Content available for download**. The Customer may download it itself during the **14 days** from the end of the Contract under Article 16 of the Terms; **on a request made within that period** the Provider will make it available **within 24 hours on working days** under Article 2.5 of the SLA. After that period the Content is retained **until the 30th day from the end of the Contract** under Article 16.2 of the Terms, solely so that the Customer can restore the Service; **if the Customer makes no choice, the Content is permanently deleted on the expiry of the 30th day.** If the Customer chooses deletion, the Processor carries it out **without undue delay** and does not wait for that period to expire. Removal from backups is governed by Article 12.3.

12.3 Backups are overwritten within the ordinary retention cycle; complete removal from backups occurs at the latest on the expiry of the retention period under Annex 2.

12.4 Data the Processor processes as a separate controller under Article 2.3, in particular billing documents, is retained for the period laid down by law.

Article 13 - Audit and demonstrating compliance

13.1 The Processor will provide the Customer with **the information needed to demonstrate compliance with the obligations** under Article 28 GDPR, normally by providing documentation of the measures under Annex 2, by answering a security questionnaire, or by submitting reports and certifications where it holds them.

13.2 If the Customer shows that the approach under Article 13.1 is insufficient in the given case, the Processor will allow an **audit** carried out by the Customer or by an auditor it has mandated. The audit is carried out **remotely**, unless the Customer shows that even that form is insufficient.

13.3 **Scope.** The audit concerns solely the processing under this DPA and the systems and premises involved in it. The Processor **is not obliged to make available**, in particular: the data and Content of other customers, third parties' confidential information, its own know-how and source code, security information whose disclosure would weaken data protection, and commercial, accounting and personnel documents unrelated to the processing. Physical access to the data centre is governed by the rules of its operator; the Processor will assist to the extent those rules permit.

13.4 An audit takes place **at most once a year**, by written agreement, on at least 30 days' notice, within working hours and in a manner that does not disrupt operations. **After a demonstrated incident or on the instruction of a supervisory authority** an audit is allowed more often too, and without the conditions under Articles 13.1 and 13.2.

13.5 The auditor must not be a competitor of the Processor and will conclude a **confidentiality agreement** with it before the audit begins.

13.6 The costs of the audit are borne by the Customer; the costs of the Processor's own assistance are borne by the Processor. Where the assistance calls for disproportionate effort, the Processor may charge for it **according to the time actually spent**, consistently with Article 9.3.

Article 14 - Liability

14.1 The parties' liability is governed by Article 82 GDPR and otherwise by Articles 32 and 33 of the Terms, including the limitation agreed there.

14.2 The Customer is liable to the Processor for harm caused by the processing having no legal basis or by the Customer having breached its obligations as controller.

Article 15 - Duration and changes

15.1 The DPA takes effect together with the Contract and lasts for as long as the Processor processes personal data for the Customer.

15.2 The provisions on confidentiality and on the fate of the data survive its termination.

15.3 Changes to the DPA are governed by Article 40 of the Terms.

Article 16 - Final provisions

16.1 The DPA is governed by the law of the Czech Republic. This is without prejudice to the application of the GDPR.

16.2 If any provision is invalid, the remainder stays in force.

16.3 Annexes 1 and 2 form an integral part of the DPA.

Annex 1 - Specification of the processing

Subject matter: providing hosting and related Services under the Contract, that is, the Services under Article 2.4 of the Terms in which the Processor stores or makes available the Customer's Content. Data processed for the Processor's own purposes under Article 2.3 is not included.

Duration: for the term of the Contract and for the period under Article 12.

Nature and purpose: storing, making available, transmitting and backing up the Content.

Types of personal data are determined by the Customer through what it stores in the Service. Typically:

- identification and contact data (first name and surname, e-mail, telephone, address)
- the content of e-mail correspondence including attachments
- data from the databases of web applications (registrations, orders, forms)
- files uploaded by the Customer or by visitors to its website
- IP addresses and other data in operational logs
- login credentials of users of the Customer's applications

Categories of data subjects: visitors and registered users of the Customer's websites and applications, the Customer's employees and collaborators, its customers and business partners, and the recipients and senders of e-mail correspondence.

Annex 2 - Technical and organisational measures

Encryption

- The servers' storage media are **encrypted**.
- **The backups are encrypted as well.**
- Data in transit is protected by TLS; SSL certificates are part of the Service.

Access control

- Access is held by the operator and by authorised collaborating persons bound by confidentiality.
- The principle of least privilege is applied.

Physical security

- The servers are in a data centre within the EU with controlled physical access.
- Encryption of the media limits the impact of unauthorised physical access.

Availability and recovery

- Automatic **daily backups of hosting accounts, retention 14 days**. What is backed up is the data needed to run the websites, applications and e-mail on the Service; data unrelated to that operation is not

covered by the backups (Articles 22.2 and 22.6 of the Terms).

- The backups are on a physically separate server and encrypted. **They are not geographically separated** - they are in the same data centre as production, so they do not protect against the failure of the whole site.
- **Virtual servers (VPS), Raspberry hosting, hosted apps and dedicated servers are not backed up**; backing them up is a matter for the Customer, in line with Article 22.4 of the Terms.
- Availability monitoring and DDoS protection run on our own infrastructure.

Integrity and confidentiality

- Separation of individual customers' data at the level of cPanel accounts and virtualisation.
- The procedure on a personal data breach under Article 11.