

HOSTZONE s.r.o.

Acceptable use policy

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/acceptable-use/>

Article 1 - Purpose and scope

1.1 This policy (the “AUP”) sets out how the Services may be used and what conduct is not permitted. It forms an integral part of the Contract under Article 3.2 of the Terms.

1.2 The AUP applies to the Customer and to everyone the Customer allows to use the Service. **The Customer is responsible for the conduct of its users** as for its own.

1.3 Terms not defined here have the meaning given in the Terms.

1.4 The purpose of the AUP is not to restrict content beyond what is necessary, but to protect other customers, the infrastructure and the Provider from the consequences of unlawful conduct.

Article 2 - Prohibited content

2.1 The Service must not be used to store, make available or distribute content that:

- is unlawful under the law of the Czech Republic or of the European Union,
- depicts **child sexual abuse** or is otherwise connected with the sexual abuse of children,
- is **terrorist** in nature or incites terrorism,
- incites violence or hatred against a group of persons or an individual,
- infringes **copyright, trade mark rights** or other intellectual property rights,
- unlawfully interferes with personality rights or the protection of personal data,
- serves **fraud, phishing** or other deception of users,
- contains **malware**, exploits or tools designed for unauthorised access to other systems,
- offers **warez**, cracks, counterfeits, or goods and services whose offering is prohibited.

2.2 **Adult content is permitted** provided it complies with the law. The Customer is responsible for meeting the obligations that attach to such content, in particular the protection of minors.

2.3 The Provider **does not monitor** the Customer's content and is under no duty to seek it out actively. It acts only upon a report or its own discovery.

Article 3 - Prohibited conduct

3.1 The following is prohibited in particular:

- **sending unsolicited communications (spam)** in any form,
- running **open relays, open proxies** and **Tor exit nodes**; a VPN for the Customer's own use is not prohibited,
- **port scanning**, penetration testing and other attempts to access systems belonging to others without their operator's demonstrable consent,
- carrying out or taking part in DoS and DDoS attacks and running botnet command-and-control servers,
- **forging headers** of e-mail messages, IP addresses or the sender's identity,

- circumventing the Service's technical limits and the Provider's measures,
- conduct that endangers the stability or security of the Provider's infrastructure or that of third parties.

3.2 The Service's storage is intended for running the Customer's websites, applications and e-mail. With Services in a shared environment (Article 21.1 of the Terms), data unrelated to that operation - in particular archives and backup copies from other systems - **is not covered by the backups** (Article 22.6 of the Terms); Article 22.3 of the Terms and Article 12 of the SLA do not apply to restoring such data. With virtual servers (VPS), Raspberry hosting, hosted apps and dedicated servers, where the Customer takes the backups itself (Article 22.4 of the Terms), **storing backup and archive data is expressly permitted**.

3.3 Running **file-sharing portals, streaming portals** and similar services whose main purpose is the mass distribution of files is prohibited.

3.4 **Game servers** are permitted on virtual servers (VPS), Raspberry hosting and dedicated servers.

Article 4 - Electronic mail

4.1 With Services in a shared environment (Article 21.1 of the Terms) the number of messages that may be sent is limited **per domain and hour** and varies with the plan chosen:

Plan	Messages per hour per domain
Pro hosting X8	100
Pro hosting X16	150
Pro hosting X32	200
Pro hosting X64	250
Pro hosting X128	300
Pro hosting X256	350
Pro hosting X512	400
Pro hosting X768	450
Pro hosting X1024	1000
Pro hosting X1536	1500
Pro hosting X2024	2000
Pro hosting X3072	3000

Where the Customer has several domains on one plan, the limit in the table applies **to each of them separately**. Messages above the limit will not be sent. Bulk sending is what a dedicated service is for, not hosting.

With virtual servers (VPS), Raspberry hosting, hosted apps and dedicated servers, where sending is handled by the Customer's own software, **the limit in the table does not apply**. **Articles 4.2 to 4.4 apply**

equally to all Services and, where abuse is suspected, the Provider may suspend sending under the procedure in Article 7.

4.2 Bulk sending of commercial communications is permissible **only to the Customer's own database of recipients who have consented to it (opt-in)**. **Purchased, rented or otherwise acquired address lists are prohibited.**

4.3 Every commercial communication must contain a working and straightforward way to unsubscribe and must identify the sender.

4.4 The Customer is responsible for the reputation of the IP addresses it sends from. Repeated blocklisting caused by the Customer's conduct is a breach of the AUP.

Article 5 - System resources

5.1 Shared hosting is an environment shared by several customers. The Customer uses resources so as not to restrict the others.

5.2 The resources allocated to an account vary with the plan chosen and the Provider enforces them technically at the level of the individual account; the Customer can see them in cPanel. The detail is set out in **Article 21 of the Terms**.

5.3 **Cryptocurrency mining and similar computationally intensive activities** are prohibited on shared hosting. On virtual servers (VPS), Raspberry hosting and dedicated servers they are permitted provided they do not restrict other customers or the infrastructure.

5.4 **SSH access** is permitted on shared hosting in a restricted environment (cPanel jail).

5.5 The procedure before the Service is restricted, and the conditions for acting without prior warning, are set out in **Article 21.4 of the Terms**.

Article 6 - Security of the Customer's applications

6.1 The Customer keeps its applications, their extensions and its passwords **up to date and secure**.

6.2 A neglected application that becomes a source of spam, malware distribution or attacks is a breach of the AUP even if it happened without the Customer's knowledge.

6.3 The Provider may alert the Customer to a vulnerability it has found; no duty to check applications follows from this.

Article 7 - Procedure on a breach

7.1 If the Provider finds a breach of the AUP, it will call on the Customer to put it right and set a period of **48 hours**, unless the nature of the breach calls for a different one.

7.2 If it is not put right, the Provider may **suspend** the Service. If the breach continues after that, it may terminate the Contract under Article 15 of the Terms.

7.3 Where the content or conduct is **manifestly unlawful**, the Provider may **suspend the Service or the content concerned immediately and without prior warning**.

7.4 For every measure under this Article the Provider gives the Customer a **statement of reasons under Article 17 of Regulation (EU) 2022/2065**, at the latest at the moment the measure takes effect. The statement describes the measure, the facts relied on, the legal or contractual basis, and the avenues of redress.

7.5 A measure under this Article gives rise to no claim to a refund of the price paid for the period during which the Service was suspended for a breach of the AUP.

7.6 If the measure turns out to have been unfounded, the Provider **restores the Service without delay**.

Article 8 - Reporting breaches

8.1 A breach of this policy may be reported through the content reporting form or at **abuse@hostzone.eu**.

8.2 The procedure after a report is received follows Article 16 of Regulation (EU) 2022/2065: receipt is acknowledged, the report is assessed by a human without automated decision-making, and the reporter is notified of the outcome.

Article 9 - Changes to this policy

9.1 Changes to the AUP are governed by Article 40 of the Terms.

9.2 A change that means a **substantial tightening** for the Customer will be notified by the Provider at least **30 days in advance**, and within that period the Customer may terminate the Contract.