

Data Processing Agreement (DPA)

pursuant to Art. 9 of the Swiss Federal Act on Data Protection (FADP) and Art. 28 of the General Data Protection Regulation (GDPR)

between the customer (hereinafter the “controller”) and FireStorm ISP GmbH, Kirchenrainstrasse 27, 8632 Tann, Switzerland (hereinafter “FireStorm” or the “processor”)

Version October 2026

1. Subject matter and duration

- 1.1 This Agreement governs the processing of personal data which FireStorm processes on behalf of the controller in the context of the agreed services (main contract), in particular web hosting, e-mail services, vServers, root servers, dedicated servers, storage and backup services, and domain and DNS services.
- 1.2 The duration of this Agreement corresponds to the duration of the main contract. Termination of the main contract also terminates this Agreement; the obligations under clause 12 (return and deletion) and confidentiality continue to apply thereafter.
- 1.3 This Agreement supplements the General Terms and Conditions (GTC) of FireStorm. In matters of data protection, this Agreement takes precedence over the GTC.

2. Nature, purpose and scope of processing

- 2.1 FireStorm provides the controller with the infrastructure for storing and processing its data (hosting, servers, storage, backup, network). Processing comprises in particular the storage, backup, transmission, restoration and deletion of data, exclusively for the provision of the agreed services.
- 2.2 The type of personal data and the categories of data subjects are determined solely by the controller through its use of the services. These may include personal master data, communication data, contract data, log data and, depending on the controller's application, sensitive personal data (e.g. health data). Data subjects may in particular be customers, patients, employees and suppliers of the controller.
- 2.3 With vServers, root servers and dedicated servers, the controller manages the operating system, applications and data itself. FireStorm has no access credentials to these systems and does not access the data stored therein. Processing by FireStorm is limited to operating the infrastructure and creating and retaining the agreed backups. Dedicated servers have no backup function; the controller is solely responsible for backing up their data.

3. Place of processing

- 3.1 Data from web hosting, e-mail services, vServers, root servers and dedicated servers, as well as all backups and snapshots, are stored and processed exclusively in data centres in Switzerland.
- 3.2 For geo-redundant name resolution, FireStorm additionally operates DNS servers at locations in Germany and France. Only DNS zone data (domain names, IP addresses and other DNS records) are stored there, no content from hosting, e-mail or servers. According to Annex 1 of the Data Protection Ordinance (DPO), these states have an adequate level of data protection.
- 3.3 For third-party products that the controller obtains via FireStorm (e.g. domain names, SSL certificates, Microsoft 365), the places of processing stated in Annex 2 apply.
- 3.4 Administration and support are carried out by FireStorm employees in Switzerland. External manufacturer support services (e.g. software or hardware manufacturers) receive, in individual

cases and insofar as necessary to resolve a fault, time-limited and monitored access to the infrastructure, but never to data within vServers, root servers and dedicated servers.

4. Instructions of the controller

- 4.1 FireStorm processes personal data exclusively within the scope of the main contract, this Agreement and the documented instructions of the controller, unless FireStorm is required to process them by Swiss law. In that case, FireStorm informs the controller of these legal requirements in advance, insofar as permitted by law.
- 4.2 The controller issues instructions by ticket or in writing. If FireStorm considers that an instruction infringes data protection provisions, FireStorm informs the controller without delay and may suspend execution until the instruction is confirmed or amended.
- 4.3 Instructions going beyond the agreed scope of services are charged according to time spent.

5. Obligations of FireStorm

- 5.1 FireStorm maintains the confidentiality of personal data. All employees with access to the infrastructure are bound to secrecy in writing, also beyond the end of the employment relationship, and receive regular training in data protection and information security.
- 5.2 Copies of data are not made without the knowledge of the controller. This excludes the agreed backups and copies that are technically necessary for proper operation.
- 5.3 FireStorm discloses personal data only where there is a legal obligation or an order of a competent Swiss authority or a Swiss court. To the extent permitted by law, FireStorm informs the controller in advance. Requests from foreign authorities are answered only by way of mutual legal assistance.
- 5.4 Mr Christian Geissler has been appointed as FireStorm's data protection advisor (support@firestorm.ch, 0844 300 200). Any change will be communicated to the controller.

6. Technical and organisational measures

- 6.1 FireStorm takes the technical and organisational measures described in Annex 1 to ensure data security appropriate to the risk in accordance with Art. 8 FADP and Art. 32 GDPR.
- 6.2 The measures are reviewed regularly and adapted to the state of the art. The level of protection must not fall below the agreed level. FireStorm notifies the controller of material changes.
- 6.3 The controller is itself responsible for security within vServers, root servers and dedicated servers (operating system, applications, access credentials, encryption of application data).

7. Notification of data security breaches

- 7.1 FireStorm informs the controller without delay, as a rule within 24 hours, after a data security breach in FireStorm's infrastructure (virtualisation platform, storage and backup systems, customer panel, network) has been confirmed that could affect the controller's data.
- 7.2 The notification contains, insofar as known, the nature of the breach, the systems and data categories affected, the likely consequences and the measures taken or proposed. Information not yet known will be provided on an ongoing basis.
- 7.3 FireStorm supports the controller in fulfilling its notification obligations towards the FDPIC (Art. 24 FADP) or the supervisory authority (Art. 33 and 34 GDPR), in particular with logs and timestamps.
- 7.4 If FireStorm detects suspicious traffic from the controller's systems, for example attacks on third parties or spam, FireStorm informs the controller. There is no obligation to monitor the controller's systems.

8. Assistance to the controller

- 8.1 If a data subject contacts FireStorm directly, FireStorm forwards the request to the controller without delay.
- 8.2 FireStorm supports the controller, to a reasonable extent, in fulfilling the rights of data subjects and in data protection impact assessments. Efforts going beyond the provision of existing information are charged according to time spent.

9. Sub-processors

- 9.1 The sub-processors engaged at the time of conclusion of the contract are listed in Annex 2. By concluding this Agreement, the controller consents to their engagement.
- 9.2 FireStorm engages new sub-processors who obtain access to data from hosting, e-mail, servers or backups only with the prior written consent of the controller. Consent may be given by e-mail and may be refused only for good cause under data protection law.
- 9.3 For third-party products (domain names, SSL certificates, Microsoft 365 and comparable products), consent to the respective provider is deemed given upon ordering the product. FireStorm informs the controller in advance of any change of these providers; the controller may object.
- 9.4 FireStorm selects sub-processors carefully and contractually imposes on them obligations corresponding to this Agreement.
- 9.5 Purely ancillary services without access to personal data, in particular space, power, cooling, physical security and network connectivity provided by data centre operators, do not constitute sub-processing. They are listed in Annex 2 for the sake of transparency.

10. Audit rights

- 10.1 Upon request, FireStorm provides the controller with the information necessary to demonstrate compliance with this Agreement.
- 10.2 The controller is entitled to audit compliance with this Agreement itself or through a third party bound to secrecy, by prior appointment (as a rule at least 14 days in advance) during business hours. Audits must not impair the operation and security of other customers. FireStorm's efforts are charged at the hourly rates applicable at the time.

11. Obligations of the controller

- 11.1 The controller is solely responsible for the lawfulness of the data processing and for safeguarding the rights of data subjects.
- 11.2 The controller informs FireStorm without delay if it detects errors or irregularities in the processing.

12. Return and deletion

- 12.1 Until the end of the contract, the controller may export its data itself at any time, and in the case of servers with full root access also as a complete image. On request, FireStorm assists the controller in this regard, charged according to time spent.
- 12.2 No later than 30 days after the end of the contract or after approval by the controller, FireStorm deletes all data of the controller, including servers, data carriers, snapshots and backups, unless a statutory retention obligation precludes this. On request, FireStorm confirms the deletion in writing.
- 12.3 The data are stored in encrypted form on the data carriers. Defective or decommissioned data carriers are professionally erased or physically destroyed before disposal.

13. Liability

- 13.1 Liability is governed by the provisions of FireStorm's GTC (in particular clause 12).
- 13.2 In relation to the data subject, the controller is responsible for damage suffered by a data subject as a result of unlawful or incorrect data processing. Recourse by the controller against FireStorm is permissible only if FireStorm has breached this Agreement intentionally or through gross negligence.
- 13.3 Contractual penalties are excluded.

14. Special right of termination

- 14.1 In the event of serious breaches by FireStorm of this Agreement, in particular of applicable data protection provisions, the controller may terminate the main contract for the services concerned without notice. In the event of insignificant breaches, the controller shall first set a reasonable deadline for remedy.

15. Final provisions

- 15.1 Both parties shall treat as confidential all knowledge of business secrets and data security measures of the other party obtained in the context of this Agreement, also beyond the end of the contract.
- 15.2 No additional fee is charged for this Agreement, unless expressly provided otherwise.
- 15.3 Amendments and supplements must be made in writing; e-mail is sufficient. Individual agreements with individual controllers take precedence over this Agreement.
- 15.4 Should individual provisions be invalid, the validity of the remaining provisions shall remain unaffected. They shall be replaced by a valid provision that comes closest to the economic purpose.
- 15.5 Swiss law applies exclusively. The place of jurisdiction is Hinwil.
- 15.6 Terms are used within the meaning of the FADP; where the GDPR applies, within the meaning of the GDPR.

Annex 1: Technical and organisational measures

Physical security (physical access control)

- Operation of the servers in ISO/IEC 27001-certified data centres in Switzerland
- Access only for authorised persons, round-the-clock monitoring of the data centres
- Redundant power supply and network connectivity
- Backup servers in a separate data centre in Switzerland

Access control and access authorisation

- Administrative access to the infrastructure by FireStorm's own employees in Switzerland; external manufacturer support only in individual cases, time-limited and monitored
- Management interfaces of the virtualisation and backup platform are not directly accessible from the Internet
- Two-factor authentication available for the customer panel
- No FireStorm access credentials to customers' vServers, root servers and dedicated servers; access credentials are set by the customer
- Logging of actions at platform level (console access, start and stop, snapshots, backups, restores) with user and timestamp

Encryption and separation

- Encrypted storage of data on the data carriers
- Encrypted transmission (TLS) for the customer panel, e-mail services and administration
- Logical separation of customers through separate virtual machines or separate hosting accounts

Availability and resilience

- Daily backups to separate backup systems, not accessible from the customer systems (included: daily backup with several restore points from the last week; more frequent backups and longer retention at extra charge). Dedicated servers have no backup function.
- DDoS protection at network level, upstream firewall with basic WAF
- Round-the-clock monitoring of the systems, fault service 24/7

Integrity and maintenance

- Installation of manufacturers' security updates for the infrastructure promptly, at the latest as soon as a patch is available
- Professional erasure or physical destruction of defective and decommissioned data carriers

Organisation

- Written confidentiality undertaking by all employees
- Employees with personal ISO/IEC 27001 Foundation certification
- Appointed data protection advisor
- Professional liability insurance for IT and telecommunications service providers, including cyber cover

Annex 2: Sub-processors and service providers

For all products

- Data centre operators in Switzerland (colocation, ISO/IEC 27001): space, power, cooling, physical security and network connectivity. No logical access to systems or data. Not a sub-processor within the meaning of clause 9.5; details available on request under confidentiality.

For DNS services only

- DNS servers at locations in Germany and France (geo-redundancy). Only DNS zone data are stored.

Only upon ordering the respective product

- Domain names: the registries and registrars responsible for the respective domain extension (e.g. SWITCH for .ch and .li, DENIC for .de, nic.at for .at, ICANN-accredited registrars). The domain holder data are processed.
- SSL certificates: the respective certification authority and its distribution partners. The certificate application data are processed.
- Microsoft 365: Microsoft and the distributor Pax8. Microsoft's privacy provisions apply.