FireStorm ISP GmbH, Kirchenrainstrasse 27, 8632 Tann

Annex 2 to the order according to Art. 28 DS-GVO: Technical and organizational measures pursuant to Art. 32 DS-GVO and Annex

Version March 2019

1. Confidentiality

Access control

- **Data centers**
    - Electronic access control system with logging
    - High security fence around the entire data center park
    - Documented key allocation to employees and colocation clients for colocation racks (each client exclusively for his colocation rack)
    - Guidelines for the escort and identification of guests in the building
    - 24/7 staffing of the data centers
    - Video surveillance at entrances and exits, security gates and server rooms
    - The access for external persons (e.g. visitors) to the rooms is limited as follows: only in company of a FireStorm ISP GmbH employee
- **Administration**
    - Electronic access control system with logging
    - Video surveillance at the inputs and outputs
- **Access control**
    - for main order "Rootserver", "Serverhousing"
        - Server passwords, which are only changed by the client after the first commissioning by himself and are not known to the contractor
        - The password for the administration interface is assigned by the client - the passwords must meet predefined guidelines.

- for main order "SiteDesigner", "Webhosting", "Mailhosting", "Reseller-hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" and all others

  - Access is password-protected, access is only possible for authorized employees of the contractor; passwords used must be of minimum length

- **Access control**

  - for internal management systems of the contractor

    - By means of regular security updates (according to the respective state of the art) the contractor ensures that unauthorized access is prevented.

    - Audit-proof, binding authorization procedure for employees of the contractor

  - for main order "Rootserver", "Serverhousing

    - The responsibility for access control lies with the client.

  - for main order "SiteDesigner", "Webhosting", "Mailhosting", "Reseller-hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" and all others

    - Through regular security updates (according to the respective state of the art), the contractor ensures that unauthorized access is prevented.

    - Audit-proof, binding authorization allocation procedure for employees of the contractor

    - For transferred data/software the client is solely responsible for security and updates.

- **Data medium control**
  - Data centers
    - Hard disks are overwritten (deleted) several times after termination with a defined procedure. After checking, the hard disks are reinstalled.
    - Defective hard disks that cannot be securely deleted are destroyed (shredded) directly in the data center.

- **Separation control**
  - for internal management systems of the contractor
    - Data is stored physically or logically separated from other data.
    - Data is also backed up on logically and/or physically separate systems.
  - for main order "Rootserver", "Serverhousing
    - Separation control is the responsibility of the client.
  - for main order "SiteDesigner", "Webhosting", "Mailhosting", "Reseller-hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" and all others
    - Data is stored physically or logically separated from other data.
    - Data is also backed up on logically and/or physically separate systems.

- **Pseudonymization**
  - The client is responsible for the pseudonymization

2. Integrity (Art. 32 para. 1 lit. b DS-GVO)

- **Forwarding control**
  - All employees are instructed in accordance with Art. 32 Para. 4 DS-GVO and are obliged to ensure that personal data is handled in compliance with data protection regulations.
  - Deletion of data in accordance with data protection regulations after completion of the order.
  - Possibilities for encrypted data transmission are provided within the scope of the service description of the main order.

- **Input control**
  - for internal management systems of the contractor
    - The data is entered or collected by the client himself.
    - Changes to the data are logged.
  - for main order "Rootserver", "Serverhousing"
    - The responsibility for input control lies with the client.
  - for main order "SiteDesigner", "Webhosting", "Mailhosting", "Reseller-hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" and all others
    - The data is entered or collected by the client himself.
    - Changes to the data are logged.

3. Availability and resilience (Art. 32 para. 1 lit. b DS-GVO)

- **Availability control**
  - for internal management systems of the contractor
    - Backup and recovery concept with daily backup of all relevant data.
    - Expert use of protection programs (virus scanners, firewalls, encryption programs, SPAM filters).
    - Use of hard disk mirroring for all relevant servers.
    - Monitoring of all relevant servers
    - Use of uninterruptible power supply, emergency power system
    - Permanently active DDoS protection
  - With main order Rootserver, Serverhousing^
    - Data backup is the responsibility of the client
    - Use of uninterruptible power supply, emergency power system
    - Permanently active DDoS protection
  - for main order "SiteDesigner", "Webhosting", "Mailhosting", "Reseller-hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" and all others
    - Backup and recovery concept with daily backup of data depending on the booked services of the main contract.
    - Use of hard disk mirroring.
    - Use of uninterruptible power supply, mains backup system.
    - Use of hardware and software firewall, web application firewall (WAF) and port regulations.
    - Permanently active DDoS protection.

- **Rapid recoverability (Art. 32 para. 1 lit. c DS-GVO);**
    - An escalation chain is defined for all internal systems, which specifies who has to be informed in case of an error in order to restore the system as quickly as possible.

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d DS-GVO; Art. 25 para. 1 DS-GVO)

- The data protection management system and the information security management system have been combined into a DIMS (Data Protection Information Security Management System).
- Incident-Response-Management is available.
- Data protection-friendly presettings are taken into account during software development (Art. 25 para. 2 DS-GVO).

- **Order control**
    - Our employees are instructed at regular intervals in data protection law and are familiar with the procedural instructions and user guidelines for data processing on behalf of the client, also with regard to the client's right to issue instructions. The general terms and conditions contain detailed information on the type and scope of the commissioned processing and use of personal data of the client.
    - The GTC contain detailed information about the purpose of the personal data of the client.
    - FireStorm ISP GmbH has appointed a company data protection officer as well as an information security officer. Both are integrated into the relevant operational processes by the data protection organization and the information security management system.