NFON
Technical and Organisational Measures Pursuant to Art. 32 Paragraph 1 Section b GDPR

Die Telefonanlage einer neuen Generation.

nfon.com

NFON

NFON AG Technical and Organisational Measures Pursuant to Article 32 Paragraph 1 Section b General Data Protection Regulation

Version 1.2

NFON AG
Machtlfinger Str. 7
81379 München
Tel.: + 49 89 45 3000
www.nfon.com

Subject to change without notice
Version 1.2/ 01.2022 (EN)
effective as of 01st January 2022

NFON

NFON AG Technical and Organisational Measures Pursuant to Article 32 Paragraph 1 Section b General Data Protection Regulation

1 Table of Contents

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

NFON AG Technical and Organisational Measures Pursuant to Article 32 Paragraph 1 Section b General Data Protection Regulation

2 Confidentiality (Art. 32 Abs. 1 lit. b General Data Protection Regulation)

2.1 Access control

Access control refers to measures suitable to “prevent unauthorised third party access to data processing equipment used to process or use personal data”.

A distinction must be made between access to the computer centres and access to the offices.

2.2 General access control measures – office access control

- Defining secured areas including determining specific measures

Based on this:

- Lock system (physical keys, chip cards, token)
- Surveillance cameras and alarm system
- Assigning rights (key management and general access authorisation)
- Visitor rules
- Rules for working in secured areas

Irrespective of secured areas

- Clear desk rules
- Delivery and despatch rules
- Visitor log
- Protecting equipment, including outside the building

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

2.3 Computer centre access control

NFON purposely does not operate its own computer centres but leases computer centre space from large providers. The computer centres hold various certifications such as ISO 27001, ITIL, eco Datacenter Five Star.

The computer centres leased are colocation services.

The general access control measures defined by NFON are also implemented by the operator of the computer centre.

Access authorisation to the computer centres are personalised and limited to a documented group of people. Authentication uses (personal) picture identification.

The data processing equipment is located inside the computer centre in separate locked racks which can only be opened with a password from NFON.

The Computer centres are solely operated in Germany using German partners.

3 Access control

Access control refers to measures suitable to "prevent unauthorised third party use of data processing equipment".

A distinction must be made between access to the computer centres, access to offices, access via the internet and general access control.

3.1 General access control

- Access rights are granted on an as needed basis. - Minimum principle
- Distinction “normal”, “privileged accounts” and “external accounts” - Role concept
- Authorisation issue and revocation process
- Regular review of authorisations
- There is a directive for locking workstation computers; clear desk policy
- Timeouts are configured according to technical possibilities.
- Mobile data storage mediums as well as the data storage mediums of laptops / notebooks are encrypted.
- All access is protected by user name and password.

- Password complexity requirements
- User activity is logged.
- Electronic and hard copy information is destroyed in compliance with data protection regulations. Destruction is documented.

3.2 Computer centre access control

- Access to the data processing equipment – after opening the rack – is further secured by user name and password.
- The group of people with access to the computer centre (racks and systems) is more limited than the group of people permitted to enter the computer centre (role assignment).

3.3 Internet access control

- Access to the data processing systems is protected by user names and passwords.
- NFON computer systems are accessed via VPN technology and personal login credentials.
- Login on the NFON computer systems at the computer centres uses SSH (Secure Shell; encrypted) and personal login credentials.
- Access to the data processing systems is generally secured by hardware firewalls.
- The NFON computer system set-up at the computer centres is minimalistic to minimise risks due to corrupt software. - System hardening
- The NFON computer systems at the computer centres undergo regular rotational system and security updates. Execution is monitored and logged by monitoring systems.

NFON AG Technical and Organisational Measures Pursuant to Article 32 Paragraph 1 Section b General Data Protection Regulation

4 Access control

Access controls are measures to "ensure those authorised to use a data processing system are only able to access data at their authorisation level, and personal data cannot be read, copied, modified or removed without authorisation during processing, use or after being saved".

In practice, access authorisations are typically linked to access rights, meaning measures to control entry also indirectly affect access.

- Access rights are granted on an as needed basis. - Minimum principle
- Distinction “normal”, “privileged accounts” and “external accounts” - Role concept
- Authorisation issue and revocation process
- Regular review of authorisations
- Access is password protected based on need for protection.
- Password complexity requirements
- User activity is logged.
- Electronic and hard copy information is destroyed in compliance with data protection regulations. Destruction is documented.

5 Separation rule

Measures to “ensure data collected for different purposes may be processed separately”.

- Separation of test and production systems
- Separate storage
  - of ERP/CRM data
  - of network profiles/configuration data
  - Service/support data of customers
- A multi-tier authorisation concept ensures different users have different rights to enter, modify and delete data in the portal interface.

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

- Logical client separation
- Definition of database rights

6 Pseudonymisation

“Processing personal data in a way so the personal data can no longer be matched to a specific person involved without additional information if this additional information is stored separately and are subject to technical and organisational measures ensuring the personal data will not be matched with an identified or identifiable individual”.

- Generating pseudonyms for given proportionality and feasibility
- Implementation of these TOMs to protect allocation information
- Central storage of allocation information

7 Integrity

7.1 Transfer control

Transfer control refers to measures suitable “to ensure personal data cannot be read, copied, modified or removed without authorisation during electronic transfer or when transported or saved to data mediums, and to review and determine at which point the transfer of personal data via data transmission equipment is scheduled".

- All employees are contractually bound to data secrecy.
- All employees are contractually bound to comply with the current legal provisions on the secrecy of telecommunications content.
- Mobile data storage mediums as well as data storage mediums of laptops / notebooks are encrypted.
- NFON computer systems at the computer centres are accessed via VPN technology and personal login credentials.
- Login on the NFON computer systems at the computer centres uses SSH (Secure Shell; encrypted) and personal login credentials.

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

- Access to the NFON data processing systems is generally secured by hardware firewalls.
- The portal interface is accessed over the internet via secured connections (SSL/TLS) with state-of-the-art key sizes.
- The deletion periods of data provided correspond with legal requirements.
- Communication with external business partners, customers and services uses state-of-the-art encryption where supported by the communication partner.
- The signatures used in encryption are validated against the certificate authority.
- Information classification specifying from which point on to encrypt.
- Logging the transmission
- Secured physical transport

7.2 Input control

Input control refers to measures suitable “to ensure the ability to subsequently review and determine if and by whom personal data systems was entered, modified or removed in data processing".

- The definition of what is being logged, particularly entering, editing and deleting data, is logged and saved for six months.
- Secure storage of log information
- A multi-tier authorisation concept ensures different users have different rights to enter, modify and delete data in the portal interface.
- The portal interfaces are accessed via individual user names and passwords.

8 Availability and capacity

8.1 Availability control and fast recoverability

Measures to “ensure personal data is protected from accidental destruction or loss".

- The computer centres hold various certifications such as ISO 27001, ITIL, eco Datacenter Five Star, dealing with the topic of availability.

- Fire protection appliances (fire extinguisher, smoke or fire detectors), no-smoking rule, water protection
- Uninterrupted power supply (UPS)
- Air conditioning
- Redundant current supply
- Extinguishing system

- Redundant internet connection for server systems
- UPS use
- Fire alarms
- Use of monitoring systems to detect errors or shortages of resources and for demand planning.
- Use of alerting systems in the event of errors, with SMS and email notification and escalation levels all the way to telephone notification via external provider.
- Use of virus protection
- 24/7 on-call service (including backup rules if unavailable)
- Live data backup via data replication at different sites.
- Failure safety through data replication and automatic failover mechanisms in the event of an error.
- Redundant computer centres with respective planning for over-capacities to fully compensate a computer centre outage by the others.
- Use of RAID systems on servers.
- Automatic daily data backup with subsequent replication on a secondary system at a different computer centre. The provision period is 12 days.
- A contingency plan / manual exists.
- Documentation of systems at a central location outside our own infrastructure.
- The software and configuration is managed via version system, allowing for quick rollbacks.
- The NFON computer systems at the computer centres undergo regular rotational system and security updates. Execution is monitored and logged by monitoring systems.
- Regular recovery drills

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

- Encrypting backups

Creating recovery plans based on internal requirements.

9 Procedure for regular review, assessment and evaluation

"Procedure for the regular review, assessment and evaluation of the effectiveness of technical and organisational measures to ensure secure processing".

- Planning audits and conducting internal and external audits
- Implementing awareness measures
- Action planning
- Reporting
- Risk management and analysis
- Proceedings for handling data breaches
- Establishing and assessing data protection related KPI
- Presets compatible with data protection

10 Order control

Measures to "ensure personal data processed as per order can only be processed as instructed by the client".

- Subcontractors are selected with care
- Thorough contract design (e.g. SLA, control rights, employee obligation, Data Protection Agreements (DPA), relevant aspects of the Telecommunications Act, etc.)
- Performing audits
- Obtaining verification (e.g. certificates)