NETWAYS®

TOM-ANNEX

Technical and organisational measures (TOM) under Art. 32 GDPR

Valid for NETWAYS GmbH and its subsidiaries

NETWAYS GmbH | Deutschherrnstr. 15-19 | 90429 Nürnberg
netways.de | Tel. +49 911 92885-0 | Fax +49 911 92885-77 | info@netways.de
Registergericht Nürnberg HRB18461 | Geschätfsführer Julian Hein, Bernd Erk
USt.-ID: DE216837402 | HypoVereinsbank | IBAN: DE52 7602 0070 0307 8013 70 | SWIFT/BIC: HYVEDEMM460

On account of the contract of order data processing according to article 28 GDPR the contracting parties commit themselves in their respective area of responsibilities and based on the contract-object, according to Art. 28 Paragraph 3 GDPR taking into account the state of the art, the cost of implantation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons the controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risks.

In detail it is concerning the following measures:

1. CONFIDENTIALITY ACCORDING TO ART.32 PARAGRAPH 1 GDPR

1.1 ENTRY CONTROL

Unauthorized persons are to be denied access to data processing systems on which personal data is processed and used.

Access to the premises is solely granted if accompanied by a NETWAYS employee, and access is only possible with personalised chipcards, if need be with biometrical verification or electronic lock with code as well as continuous camera surveillance.

A continuous perimeter protection is granted by enclosure facilities and personnel.

Separate racks are additionally secured by manual closing systems, which are managed by safes. Appropriate key regulation including access restriction is implemented.

1.2. ADMISSION CONTROL

Unauthorised persons are to be prevented from using the data processing systems.

The server- and client systems are secured by login with username and password, remote access is only granted with at least asymmetric encryption methods for terminal- and VPN- access in place. Port access to exposed services are restricted by redundant firewall systems/ network devices. Centrally managed user rights, guidelines for data protection, password quality policy, non-disclosure agreements based on industrial law and instructions on terminal usage are implemented.

1.3 ACCESS CONTROL

It is to be ensured, that the authorized persons solely access the data they are permitted to, and that any personal data may not be read, copied, modified or deleted without authorisation while being processed, used or after saving.

Encryption quality and security protocols will be implemented according to the client`s possibility. In principle server and general network services of the internet are not accessible.

The number of administrators is to be kept at a minimum, and user profiles are to be managed via a central authorisation system. Modifications can be retraced with the help of revision proof snapshots of hard disk space or by a central log- or configuration management system.

Token- and VPN access systems are protected by safe and access regulations.

Destruction and deletion according to DIN 66399 and DIN 32757 on security levels P5 and T4 on request of the client. The deletion concept can be viewed on demand.

1.4 SEPARATION CONTROL

It is to be ensured that data collected for different reasons can be processed separately.

If configuration management or virtual resources of the client are used, these have to be separated in function and tested during an evaluation and production phase.

The contractor may only store the data on his own physical options. The client is responsible for logically separating the data.

1.5 PSEUDONYMISATION (ARTICLE. 32. PARAGRAPH 1 GDPR)

Pseudomysation as a process that is required when data are stored to transform personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information as long as this additional information is kept separately from the pseudonymised data, and subjected to technical and organisational measures.

Pseudonymisation is realised on request of the client in accordance with the data transfer control (2.1) or if need be within the context of a backup (Privacy by design). Internal guidelines for pseudonymisation or anonymisation of personal data in case of a transfer are implemented.

2. INTEGRITY ACCORDING TO ART.32 PARAGRAPH 1 GDPR

2.1 TRANSFER CONTROL

It is to be ensured, that personal data being transferred, transported or stored on data carriers cannot be read, copied, modified or deleted by unauthorised persons, and that it can be inspected and determined where planned transfers of personal data will take place.

The client will get dedicated, encrypted access to his/her environment, which in some cases is run in an independent VLAN.

For one-time transport or support encrypted access will be provided, i.e. HTTPS or SFTP. Storing data on data carriers for transportation will only occur if the client requests it specifically, and, can only occur if personally delivered. Every extraordinary transportation must be arranged by the client beforehand and recorded accordingly. Furthermore, encryption and pseudonymisation can be agreed upon.

2.2 INPUT CONTROL

It is necessary to ensure the possibility to subsequently determine if and by whom personal data has been entered, modified or removed in the data processing systems.

Revision proof snapshots are taken of the hard disk space by virtual resources, server systems and containers. If needed, alterations can be retraced via a central log management system. Alterations or inputs are done by the client and are recorded accordingly.

3. AVAILABILITY AND RESILIENCY ACCORDING TO ART. 32 PARAGRAPH 1 GDPR

3.1 AVAILABILITY CONTROL

Personal data needs to be protected against accidental destruction or loss.

Server systems leased by the customer are equipped with redundant disk arrays (minimum requirement RAID1) and may be provided with a support contract from the server manufacturer. Power supply is redundantly implemented and protected against failure of the electricity supply system by UPS or generators.

The contractor hosts a data backup system which may be used by the customer in case needed. By default, a backup is created once a day, which consists of a full backup once a week and of a differential backup on the remaining days. The data backup system is distributed and may be on two different locations and is inspected on a regular basis.

Virtual server systems and containers may be secured to the above mentioned system by revision proof snapshots of the hard disk space. The retention period is 7 days.

4. PROCESSES FOR REGULAR INSPECTION, ASSESSMENT AND EVALUATION IN ACCORDANCE WITH ART. 32 PARAGRAPH 1 GDPR AND ART. 25 PARAGRAPH 1 GDPR

4.1 DATA PROTECTION MANAGEMENT

Guarantee for the sustainability of data privacy protection

Documentation of data protection policy is available and accessible to all employees if needed. Regular inspection of effectiveness of the protection measures are carried out. Employees are trained in confidentiality and are bound to data secrecy.

The client meets the information obligations in accordance with Art. 32 Paragraph 1 GDPR and Art. 25 paragraph 1 GDPR. Internal data protection commissioner: **privacy@netways.de**

4.2 INCIDENT-RESPONSE-MANAGEMENT

Support for reaction on security infringement cases

The contractor uses redundant firewall, network and spam filter systems in his environments. The functionality is guaranteed by regular inspection and maintenance. The client's projects and environments are documented, and current developments or general information are recorded in a ticket system. Security incidents are documented and a controller for data protection is being involved.

4.3 PRIVACY POLICY FRIENDLY PRE-SETTINGS (ART. 25 PARAGRAPH 2 GDPR)

Privacy by design / Privacy by default

Only personal data necessary for the respective purpose is collected, processed and used. The person affected can easily make use of his or her power of revocation.

4.4 ORDER CONTROL

Order processing as per instructions must be guaranteed.

All client instructions are given in writing by e-mail or to our ticket system, which guarantees continuous accountability. Verbal agreements are recorded in the ticket system and sent to the client for inspection. Instructions are checked for plausibility by the contractor's employees. Employees are bound by a non-disclosure agreement. All processes are inspected and evaluated regularly by the respective heads of department and the management.

The contractor guarantees a simple assertion of the client's control rights at all times, for regular inspection of the protection level.

In principle no other subcontractors are engaged unless the client explicitly wishes to.

After completion of the contract all of the client's data is either returned or deleted. A concept for deletion can be inspected on request.