CONNECTIVE

Connective - General Description of Technical and Organizational Measures

version 1.0

This document describes the Technical and Organizational Measures taken by Connective to comply with Article 32 of the General Data Protection Regulation (GDPR).

creating trust connecting value

Connective Belgium
Wapenstraat 14 B301
2000 Antwerpen
T +32 3 612 58 60
www.connective.eu

Connective France
104 Avenue Albert 1er
92500 Rueil Malmaison
T +33 1 47 10 04 67
www.connective.eu

Connective The Netherlands
Evert van de Beekstraat 360
1118 CZ Schiphol
T+31 85 888 01 08
www.connective.eu

Revisions

Date	Version	Owner	Topic
2019-08-21	0.1	Filip Verreth	Document Creation
2019-08-23	1.0	Filip Verreth	Final document

CONNECTIVE

Table of content

Preface

The 2016/679 European regulation of 27th April 2016 (known as "General Data Protection Regulation" or GDPR) specifies that protecting personal data requires taking "appropriate technical and organizational measures to ensure a level of security appropriate to the risk" (Article 32).

This document describes the Technical and Organizational Measures taken by Connective to comply with Article 32.

1. Introduction

1.1. Policies and practices

1.1.1. Organization administrating the Services

The Connective TSP Board is the authority that is responsible for this TOM Statement. The Connective TSP Board is part of Connective NV (registered under number 0467.046.486 in Belgium).

1.1.2. Contact persons

Questions about this statement should be addressed to the president of the Connective TSP Board.

This can be done via the contact form on the Connective website at https://connective.eu/about-us/trust-center/ or via e-mail at tsp-board@connective.eu or via postal mail at Connective TSP Board; Connective NV; Wapenstraat 14 bus 301, 2000 Antwerp.

GDPR related questions should be addressed to Connective's DPO Office.

This can be done via the contact form on the Connective website at https://connective.eu/about-us/trust-center/ or via e-mail at dpo@connective.eu or via postal mail at Connective DPO Office; Connective NV; Wapenstraat 14 bus 301, 2000 Antwerp.

2. Confidentiality (Art. 32 (1) (b) of the GDPR)

The risk of physical, material or immaterial damage or the risk of impaired rights and freedoms for the persons affected must be reduced.

2.1. Access control Connective's buildings

Technical and organizational measures:

- Physical access control for access to the building and offices
- Further protective measures
  - Alarm system for critical areas

2.2. Access control Connective's network

Technical and organizational measures:

- Access control to computers of the Connective network
  - User ID
  - Secure password
    - Password repetition lock after 3 failed attempts
    - Complexity, min. 8 characters, no password repetitions
    - Two-factor authentication
  - Administrative Accounts (IT and Cloud Team)
    - Two-factor authentication
    - RBAC
- Time-controlled password-protected pause circuit (screensaver)
  - A regulation exists by which employees are obligated to lock their computers manually when leaving their workstation. After 10 minutes the screen is automatically locked.
- Securing the networked systems against unauthorized intrusion
  - Firewall
  - Anti-Malware scanner
  - Auditing and threat detection
- Hard drives in personal computers are encrypted

2.3. Access control Connective's systems

Technical and organizational measures:

- Permission profile for employees
  - User administration
  - Access authority dependent on
    - Responsibilities task
  - If necessary, also differentiated according to
    - read permission
    - write permission
- Permissions for external employees are documented in the IT database. All requests for permission changes are documented by IT in the ticket system.
- Clear rules for adjusting rights management
  - When changing the area of responsibility of an employee or termination, rights that are no longer required are promptly adjusted.
  - Changes are handled and documented via the ticket system of IT.

- Permissions of external employees and access to business-critical applications are checked regularly.
- Measures for access control
  - Program review and approval process
  - Logging and evaluation of security-critical incidents
  - Changes to firewall settings

2.4. Separation control

Technical and organizational measures:

- **Connective Cloud Systems**
  - Logical separation of data (documents) and databases per controller
    - Documents: each controller has their own storage container in which to store their documents
    - Application Database: each controller has their own database
    - Connective system database
      - Contains data required for the operation of the system (not controller- specific)

3. Integrity (Article 32 (1) (b) GDPR)

The risk of physical, material or immaterial damage or the risk of impaired rights and freedoms for affected persons due to unintentional or unauthorized modification or unlawful or negligent acts upon data processed in the job must be reduced.

3.1. Transfer control

Technical and organizational measures:

- Transmission of data via the Internet is always in encrypted format
  - VPN: between different locations of the company network and datacenters
  - TLS: access to the Connective Cloud systems for controllers
- Protection of data during its transmission
  - Password protection
  - Access data (including controller systems)
    - Secrets are managed in a Secret Management system
    - Important:
      - Test accounts or access data for Connective Support or Professional Services are deactivated or the passwords changed after the support case or project has been completed
- Safeguarding of PCs and external drives (mobile hard drives, USB sticks, etc.) against misuse
  - Connective's Internal Security and Privacy Policy contains provisions regarding the use mobile devices and the use of encryption.
- Secure deletion / disposal of data carriers
  - Policies are in place

Access to the controller data and controller systems in a remote maintenance is limited to authorized personnel only and done with the prior approval of the controller.

- Logging and log evaluation during remote maintenance
  - The access is logged in our system
  - An evaluation takes place only in case of suspicion.

3.2. Input control

Technical and organizational measures

- Access to the controller data and controller systems in a remote maintenance
  - In agreement with the controller, Connective's Delivery Team sometimes also uses a mode in which the controller does not have to confirm the connection on their environment

4. Availability and Resilience (Article 32 (1) (b) GDPR)

The risk of physical, material or immaterial damage or the risk of impaired rights and freedoms for affected persons also due to unlawful or negligent acts owing to non-availability of data processed in the job must be reduced.

4.1. Availability control

Technical and organizational measures:

- Backup: Important data is regularly saved in a backup system and synchronized to an external location according to defined schedules (Cloud backup). Backups are encrypted at rest and in transit.
- Reporting channels are known.
- Continuity and recovery plans exist for central systems
  - Important servers of the Cloud systems can be set up again at any time
- Restore of central systems in IT is regularly tested

4.2. Load capacity of the systems

Technical and organizational measures:

- Connective Cloud systems
  - Important background servers can be dynamically scaled up and down at any time by launching additional servers and adding them to the Connective Cluster
  - Denial of service is ensured by Azure Basic DDOS protection

- Internal IT
  - Important background servers can be dynamically scaled up and down at any time

5. Procedure for Regular Review, Rating, and Evaluation (Article 32 (1) (d) of the GDPR; Article 25 (1) of the GDPR)

Procedures shall be followed for the periodic review, rating, and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing.

5.1. Job control

Technical and organizational measures:

- Periodic review
    - "Technical and organizational measures" are reviewed at least once a year
- Monitoring the execution of the sales order / service action
    - Connective's Delivery Team describes a User Acceptance Test before the job is executed (test plan, which must work according to the order).
- Logging and evaluation mechanisms when accessing controller systems and controller data

5.2. Internal organization

Technical and organizational measures:

- Data protection management
    - There are internal policies and a data protection policies and procedures.
    - All employees are trained and made aware of the topic of data protection at regular intervals (at least once a year).
    - Job descriptions and responsibilities are are defined and communicated within the company. This is reviewed on a regular basis by senior management as part of ETSI EN 319401 (Trust Service Provider) certification.
- Incident management
    - Compliance with the technical and organizational measures is reviewed annually (audit) by the Data Protection Office and adapted if necessary.
    - As part of certifications, the incident management is checked.

Data protection through technology design:

- Data Protection by Design (DPbD) principles are in the heart of our development process
- Selection of privacy-friendly technology during procurement
- Connective Cloud systems
    - Microsoft is continually expanding and improving its Azure Cloud Services. New services that improve data security are generally integrated into the Connective Cloud Services in a timely manner.