



Technical and Organizational Measures

17.11.2023 – v2.0

Security Appendix and Technical and Organizational Measures

This document describes Technical and Organizational Measures in place in LINK Mobility group of companies. The document is also an appendix to LINK Data Processing Agreement.

Requirement for information security

LINK, who according to the Agreement processes Personal Data on behalf of the Controller, shall implement appropriate technical and organizational measures as stipulated in Data Protection Legislation and/or measures imposed by relevant supervisory authority pursuant to Data Protection Legislation or other applicable statutory law to ensure an appropriate level of security.

LINK shall assess the appropriate level of security and take into account the risks related to the processing in relation to the services under the Agreement, including risk for accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Person Data transmitted, stored or otherwise processed.

All transmissions of Personal Data between LINK and the Controller or between LINK and any third party shall be done at a sufficient security level, or otherwise as agreed between the Parties.

This Appendix contains a general description of technical and organizational measures that should be implemented by LINK to ensure an appropriate level of security.

To the extent LINK has access to such information, LINK shall provide the Controller with general descriptions of its Sub-processors' technical and organizational measures implemented to ensure an appropriate level of security.

Technical and organizational measures

Physical access control

LINK should take proportionate measures to prevent unauthorized physical access to LINK's premises and facilities holding Personal Data.

Measures should include:

- Procedural and/or physical access control systems.
- Door locking or other electronic access control measures.
- Alarm system, video/CCTV monitor, or other surveillance facilities.
- Logging of facility entries/exits.
- ID, key, or other access requirements.
- Guest procedures.

Access control to systems

LINK should take proportionate measures to prevent unauthorized access to systems holding Personal Data.

Measures should include:

- Password procedures including requirements to:
 - length,
 - use of special characters, alphanumeric characters, uppercase and lowercase letters,
 - forced change of password on a frequent basis,
 - multi-factor authentication,
 - use of unique passwords,
 - resilience to dictionary attacks.
- Access to systems is subject to approval from the system owner.
- No access to systems for guest users or anonymous accounts.
- Central management of system access.

- Remote access procedures including requirements to:
 - use secure protocols for remote access,
 - use strong user authentication,
 - ensuring accountability of users,
 - terminating remote access sessions after fixed period of time.
- Privileged access rights procedures including requirements to:
 - approval from asset owner for granting privileged access rights,
 - separating standard user accounts from privileged access rights accounts,
- Routines of manual lock when workstations are left unattended, and automatic lock within a maximum 5 minutes.
- Restrictions on use of removable media, such as memory sticks, CD/DVD disks or portable hard drives, and requirements of encryption.

Access control to data

LINK should take proportionate measures to prevent unauthorized users from accessing data beyond their authorized access rights, and to prevent the unauthorized access to or removal, modification, or disclosure of Personal Data.

Measures should include:

- Differentiated access rights, defined according to duties.
- Automated log of user access via IT systems.
- Encryption and data masking.
- Granting access on a need-to-have basis.
- Conducting access rights reviews.

Data entry control

LINK should take proportionate measures to check and establish whether and by whom Personal Data has been supplied in the systems, modified, or removed.

Measures should include:

- Differentiated access rights based on duties
- Automated log of user access, and frequent review of security logs to uncover and follow up on any potential incidents
- Ensure that it is possible to verify and establish to which bodies Personal Data have been or may be transmitted or made available using data communication equipment
- Ensure that it is possible to verify and establish which Personal Data has been entered into data-processing systems, altered or deleted, and when and by whom the Personal Data has been input, altered, or deleted

Disclosure control

LINK should take proportionate measures to prevent unauthorized access, alteration, or removal of Personal Data during transfer of the Personal Data.

Measures should include:

- Use of state-of-the-art encryption on all electronic transfers of Personal Data
- Encryption using a VPN or HTTPS for remote access, transport, and communication of Personal Data
- Audit trail of all data transfers

Availability control

LINK should take proportionate measures to ensure that Personal Data is protected from accidental destruction or loss.

Measures should include:

- Frequent backup of Personal Data
- Remote storage
- Use of anti-virus/firewall protection
- Monitoring of systems in order to detect viruses etc.

- Ensure stored Personal Data cannot be corrupted by means of malfunctioning of the system
- Ensure that installed systems may, in the case of interruption, be restored
- Uninterruptible power supply (UPS)
- Business Continuity procedures

Separation control

LINK should take proportionate measures to ensure that Personal Data collected for different purposes are processed separately.

Measures should include:

- Restrictions on access to Personal Data stored for different purposes based on duties
- Segregation of business IT systems

Job/subcontractor control

LINK should implement measures to ensure that, in the case of commissioned processing of Personal Data, the Personal Data is processed strictly in accordance with the Controller's instructions.

Measures should include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

Training and Awareness

LINK should ensure that all employees are aware of routines on security and confidentiality, through:

- Unambiguous regulations in employment contracts on confidentiality, security, and compliance with internal routines
- Internal routines and courses on requirements of processing of Personal Data to create awareness