clearstream | DEUTSCHE BÖRSE GROUP

Data protection and data security concept

Technical and organisational measures

For customers of Clearstream Banking Luxembourg

Document number: 7236

May 2019

Unless otherwise stated, all times are given in Central European Time (CET).

Foreword

This document outlines the binding technical and organisational measures associated with commissioned data processing operations carried out between the principals and agents of Clearstream Banking Luxembourg and provides information about the valid data protection and data backup concept.

Scope

The technical and organisational measures described apply to CBL.

This page has intentionally been left blank.

Contents

Foreword **3**

1. Data protection and data security concept

2. Confidentiality

2.1 Access control 2-9
2.2 Access control to data processing systems 2-10
2.3 Access control/User control 2-11
2.4 Separation control 2-12

3. Integrity

3.1 Transmission control/Transfer control 3-13
3.2 Input control/Data storage device control/Storage control 3-14

4. Availability and resilience/recoverability

4.1 Creation and safekeeping of backups 4-15
4.2 Safeguarding of day-to-day operations 4-15
4.3 Measures for operational disaster control 4-16
4.4 Organisational measures 4-16

5. Procedure for regular monitoring, assessment and evaluation

5.1 Data protection management 5-17
5.2 Incident response management 5-17
5.3 Data protection by design and by default 5-17
5.4 Order control 5-18

1. Data protection and data security concept

The following outlines the specific technical and organisational measures implemented pursuant to Art. 24(1) of the EU General Data Protection Regulation (GDPR) for commissioned data processing.

Clearstream Banking S.A.fulfils the obligation established in the GDPR to safeguard processing of personal data by means of appropriate technical and organisational measures and, where possible, to anonymise or pseudonymise personal data. All measures implemented must take the risk associated with the respective data processing operation into consideration and be state of the art. In particular, the effectiveness of the measure should take account of the protection objectives of confidentiality, availability, integrity and capacity. This is supported by integrating data protection measures, information security and additional measures to safeguard data processing operations.

Definition of security value terms:

- **Confidentiality:** Protection of data, information and programmes against unauthorised access and disclosure.
- **Integrity:** Factual and technical accuracy and completeness of all information and data during processing.
- **Availability:** Reliable access to information and data by authorised users.
- **Resilience:** Denoted as an aspect of availability and thus the capacity of information, data, applications, IT systems and IT networks in the event of malfunction, failure or heavy use.

This page has intentionally been left blank.

2. Confidentiality

Technical and organisational measures are implemented that are appropriate for safeguarding confidentiality. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of data processing as well as the potential impact on the rights of natural persons, the following measures are taken to safeguard the confidentiality of personal data.

2.1 Access control

Measures are implemented that deny unauthorised persons access to data processing systems that process and/or use personal data. This is done by:

2.1.1 Physical security

- Business premises and buildings are monitored 24 hours a day, seven days a week by security staff.
- The data centre – and thus the hardware, server or components – is located in a separate secure area that is segregated from normal office premises.
- Opening of doors is also technically monitored.
- Inspection patrols are carried out.
- There are service contracts for technical surveillance systems.
- An identity check is carried out by security staff.
- Access is logged.
- Access is only granted to authorised persons after checking and establishing identity.

2.1.2 Security zones

The data centre is an area segregated from office premises with strictly restricted access and surveillance (closed shop).

2.1.3 Type of access control

- An automatic identity check is carried out by means of personal access cards and recording attendance using smart card readers.
- Offices are secured by a electronic card reader.
- The reception is staffed during core hours and receives visitors.
- Emergency exits are secured against improper use.

2.1.4 Regulation of access authorisation

- Access authorisation is organised restrictively and granted on the basis of appropriate authorisation procedures.
- Authorised persons are determined with respect to security areas (for example data centre).
- Visitors and externals must report to the reception desk and are collected and accompanied.
- There are rules for employees leaving the company and changes in internal jobs and/or authorisation.
- There are rules/follow-up measures if passes, keys, etc. are lost.

- Maintenance and repair staff are supervised.
- The granting and withdrawal of access authorisation is reviewed on a monthly basis by the respective line manager.

2.2 Access control to data processing systems

Use of data processing systems by unauthorised persons is prevented by:

2.2.1 Access authorisation control

- Access authorisation is granted to users on the basis of authorisation procedures.
- Personal user ID and personal initial passwords are allocated.
- Access is only granted after prior login with authentication (user ID, password or also token device).
- The screen session is automatically protected by screen savers requiring a password after a set period of time and can also be manually locked.
- Measures for password security (length, complexity and safekeeping) and rules for the use of passwords are in place.
- Rules are in place if passwords or token devices are lost or forgotten.
- A rule that makes a need-to-know and a need-to-do principle compulsory for authorisation procedures is in place.
- Administrator accounts are exclusively used for strictly limited activities.
- Rules are in place for authorised persons leaving the company or changing jobs.
- Disconnection occurs in the case of repeated failed attempts or timeouts.
- Inactive connections are automatically closed after a set waiting period (timeout).
- There is a separate infrastructure for visitors.
- Users can only have access to personal data according to the authorisation granted to them (by means of role allocation, functional user etc.).
- Personal data are securely stored in RACF (Resource Access Control Facility) inactive mode.
- Unauthorised attempted access is detected (for example logging of system use) and investigated accordingly.

2.2.2 Additional measures for remote access

- To log in remotely, a special request has to be made and approved.
- Network access security is provided by means of hardware and software measures.
- Unauthorised access from the internet is prevented by use of firewalls.
- Unauthorised attempted access can be detected (intrusion detection).
- Protection of existing sessions against takeover by other users (session hijacking) is provided.

2.2.3 Logging of access

- Access to data processing systems and workstations is logged (for example in a log file).
- Use of data processing systems is verifiable (logging of access).
- Remote access via the (SSL) VPN gateway is logged.

- The granting/changing of access authorisation is logged.
- Logs are regularly evaluated.

2.3 Access control/User control

To ensure that authorised persons can only access the data covered by their access authorisation when using a data processing system and that personal data are not read, copied, altered or deleted without authorisation when processing, using and after storing personal data, the following measures are in place:

2.3.1 Authorisation concept

- Rules are established for granting and managing access authorisation.
- Individual access rights and user groups have been formed.
- User groups are managed in a central directory service.
- Granted authorisation is regularly reviewed.

2.3.2 Access control

- Confidentiality of data is ensured by using encryption and key management routines in line with industry standards.
- For data in transit a TLS session is established between the browser and web server. Commercial strength 256-bit keys are used for the encrypted session.
- Data centres are protected by the highest level of physical security in line with industry standards.
- Business applications on mobile devices are encrypted.
- Network access security has been set up.
- Only approved hardware and software are used.
- Network components are protected.
- The network is segregated.
- There is separation between testing and productive environments.
- Critical services are subject to monitoring.
- Database access is restricted applying a need-to-have approach.
- The secure disposal of information (certified in accordance with DIN 66399) is guaranteed.

2.3.3 Safekeeping when using data storage devices

- The safekeeping of data storage devices is controlled.
- Encrypted data storage devices are available.
- Data storage devices are not repaired, but rather are subject to more secure deletion/destruction (in accordance with DIN 66399).
- Persons authorised for data storage device removal are specified.
- Hard drives are hardware encrypted.

2.4 Separation control

The following measures are in place to ensure that data collected for different purposes can be processed separately:

- The software and filing structure used are able to support multiple principals.
- Logical separation of data is established.
- Internal guidelines for data collection and processing are established.

3. Integrity

Factual and technical accuracy and completeness of all information and data during the processing of personal data are guaranteed. The identification and correction of unauthorised modifications must be ensured. The following checks ensure the integrity of personal data:

3.1 Transmission control/Transfer control

Unauthorised reading, copying, alteration or deletion in the case of electronic transfer or transmission should be prevented. This is done as follows:

3.1.1 Regulation concerning electronic transfer

- Data transfer takes place in protected networks.
- External networks are used exclusively (VPN, dedicated line).
- Filter mechanisms prevent connections to/from unauthorised IT systems (firewall).
- There is the option of encrypting data (for example S-MIME, PGP) and transferring encrypted data (for example SSL, TLS).
- Emails are authenticated (digital signature).

3.1.2 Regulation concerning storage on removable media

In principle, storage of personal data on removable media is not provided. In exceptional cases, only encrypted mobile data storage devices are used:

- Personal data are exclusively stored and held on data storage devices (tapes or USB sticks, etc.) in a central data centre with secured access.
- In principle, private data storage devices are prohibited on business premises; case-specific exceptions are only approved on request.

3.1.3 Regulations concerning the transportation of data storage devices

- Data storage devices containing personal data are protected against unauthorised access, damage and loss during transportation.
- Data storage devices containing personal data are transported exclusively by in-house messengers, under secure transportation conditions or using another secure form of dispatch.
- Data storage devices are encrypted.
- Paper is disposed of by means of document shredders and/or disposal firms.

3.1.4 Regulations concerning the disposal of data storage devices

Data storage devices are disposed of in accordance with data protection requirements and destroyed by the disposal firm.

3.2 Input control/Data storage device control/Storage control

To ensure that it can be subsequently checked and established whether and by whom personal data is entered, altered or deleted in data processing systems, the following measures are in place:

- Responsibilities for data entry, including stand-in arrangements, are established by assigning authorisation.
- Logging of all entries, alterations or deletions of data so that the originator, time and content of the change can be traced.
- Relevant user activities are recorded (sender, time stamp and change content).
- Log evaluation systems analyse captured logs.

4. Availability and resilience/recoverability

It should be guaranteed that personal data are protected against the risk of accidental destruction or loss. To this end, the following measures have been implemented:

4.1 Creation and safekeeping of backups

- A documented data backup concept is available.
- Controlled and regular backup of files and databases.
- Testing of data backup is regularly carried out and documented.
- Data backup is protected against unauthorised access.
- Backup disks are securely stored separately from the original data at specially protected locations.

4.2 Safeguarding of day-to-day operations

Day-to-day operations are secured by means of the following technical and organisational measures:

- Shift operation
- Capacity planning and monitoring

4.2.1 Resilience

Completely redundant Sysplex (System processing complex) (at least 99.9% availability)

4.2.2 Uninterruptible power supply

- An uninterruptible power supply (UPS) with sufficient capacity is installed upstream of the data centre.
- Proper functioning is ensured by means of regular testing.
- Tests are documented.

4.2.3 Fire protection

- Area-wide fire alarms and/or early fire detection devices are available (depending on location).
- CO_2 handheld fire extinguishers are available in the data centre.
- A reduction of the fire load is taken into account.

4.2.4 Air-conditioning

- Redundant air-conditioning systems are present in the data centre.
- Multiple climate control modules are present for optimal cooling distribution.
- Leakage warnings and temperature monitoring are relayed to the permanently manned security control room.
- Responsible employees (IT Operations, IT Management) are notified by the security personnel if triggered.

- Service contracts are in place.

4.2.5 Internet connection

A redundant internet connection is available.

4.3 Measures for operational disaster control

- A Disaster Recovery Manual (with responsibilities) has been prepared and is maintained.
- Emergency organisation is in place.
- Emergency drills are carried out and documented.

4.4 Organisational measures

- Security guidelines as well as security and privacy operating procedures exist, have been announced and are checked.
- There are requirements for procedural and programme documentation.
- The hardware and software used are available and ready for operation in order to produce the original data from copies using backup devices.
- Operational availability is regularly checked.
- Before being put into operation, IT systems are finalised according to defined procedures and thus raised to a higher security level.
- Business Continuity Management is in place.
- A failover procedure has been defined.
- There are sufficient staff resources available.
- Users are trained.
- An information security officer has been appointed.
- There are rules for file retention (central backup).
- Data are only deleted at the end of the defined retention periods.

5. Procedure for regular monitoring, assessment and evaluation

The effectiveness of the measures implemented must be reviewed, assessed and evaluated by means of internal processes and procedures, especially at organisational level.

5.1 Data protection management

The extensive obligations and requirements of the GDPR call for a comprehensive strategy based on a structured approach and an appropriate management system. All the components necessary for ensuring data protection are subject to systematic coordination of data protection management. This includes the following measures:

- Data protection organisation has been established.
- A structured approach is followed via the data protection strategy.
- Established processes provide for the involvement of the data protection officer.
- Privacy guidelines and operating procedures have been announced and compliance is monitored.
- There are formalised approval procedures for new data processing procedures and in the case of significant changes in legacy processes.

5.2 Incident response management

Relevant reporting channels should be defined and responsibilities established to be able to respond to an incident, if necessary. To this end, the following measures have been implemented:

- Employees are trained accordingly.
- Points of contact and channels have been defined for (security-related) incidents.
- An organised approach has been adopted.
- Documentation is maintained.
- Experience gained is channelled into the further design and improvement of processes.

5.3 Data protection by design and by default

Default settings ensure that personal data are only processed in accordance with the specific processing purpose. This applies to the quantity of personal data collected, the scope of processing, the retention period and accessibility. The following measures have been implemented:

- Thanks to the ongoing awareness and training process within the context of data protection management, employees are careful when handling personal data and consider the privacy principle of data minimisation to be part of the development of technical and business processes.

5.4 Order control

It is ensured that commissioned personal data processing is only carried out in accordance with the principal's instructions. Commissioned data processing as defined in Art. 28 of the GDPR is not carried out without the principal's appropriate instruction. To this end, the following measures have been implemented:

- An internal process ensures that the necessary contracts for commissioned data processing are completed.
- A written contract between principal and agent is available in each case.
- The principal issues written instructions to the agent.
- The agent has ensured adequate internal rules as a result of the commission and the principal's related instructions.
- Sufficient measures to ensure compliance with data protection by a possible subagent can also checked by the principal.
- If an inspection has been carried out by the regulatory authority at the agent, the principal may request the inspection report; the same applies to inspections at possible subagents.

Contact

www.clearstream.com

Published by

Clearstream Banking Luxembourg

Registered address
Clearstream Banking S.A.
Luxembourg
42 Avenue JF Kennedy
L - 1855 Luxembourg

Postal address
Clearstream Banking S.A.
L-2967 Luxembourg

May 2019

Document number: 7249