Technical and Organisational Measures, Art. 32 sec. I GDPR

Applicable for the Frankfurt location of:

CACEIS Bank S.A., Germany Branch and

CACEIS Fond Services GmbH

V. 1.1, updated September 2020

1 CONFIDENTIALITY (ARTICLE 32 SECTION 1 LIT. B GDPR)

1.1 Physical Access Control

Personal access control is realized through the following measures:

a) Buildings and external areas are controlled by security personnel.
b) Alarms are in place.
c) The building entrance is protected by an intercom system.
d) External persons may only obtain access to the premises with an employee sponsor and have to be accompanied until the end of their visit.

1.2 Electronic Access Control

To prevent the unauthorized use of computer systems of CBG, the following measures have been established:

a) Access to computer systems is regulated by individual access identification and associated passwords.
b) The CBG security policy defines password rules. These rules are implemented.
c) The assigned User IDs are up-to-date: following the procedure for on-boarding / change of department / off-boarding of employees.
d) Screen locking routines are used;
e) Firewall environment works with different virtual LANs: There are several virtual LAN segments, one is the *demilitarized zone* (“DMZ”). The redundancy of the DMZ is ensured.
f) The USB ports are blocked by default. On individual request users can request the activation of the USB port. IT is mandatory to consult the CBG Chief Information Security Officer (“CISO”) for the approval of such requests.

1.3 Internal Access Control (permissions for user rights of access to and amendment of data)

It must be guaranteed that the persons authorized to use a data processing system can access only the data permitted by their task assignment.

a) The provisioning process is formalized.
b) The provision of access permissions is done independently from the business units.
c) All systems used have adequate access control measures in place. The systems’ access control measures are part of the security concept of the systems that is regularly checked.
d) The “need to know” is ensured by the concept of the “business profiles”: A business profile is the description of all access rights needed for a specific task. Users are assigned to business profiles, rather than directly to system access rights.
e) The business profiles are managed by a central access management unit that is using the User Management System (“UMS”) based on Oracle solution.
f) Change of “business profile” permission follow a strict process:
The business department issues the request to user management team. The business application responsible and the risk department are involved in the approval process (Requests and approvals are traced).
g) Complete check of toxic access right combination is performed regularly to ensure that conflicted or toxic is prohibited.
h) For every business profile change, the toxic access right combinations are checked by the Risk department.
i) Regular checks to ensure that the system’s authorisations comply with the defined authorisations (reconciliation).
j) Regular checks to ensure that the content of “business profile” is correct (recertification).

1.4 Pseudonymisation/Anonymisation (Article 32 Section 1 lit. A GDPR; Article 25 Section 1 GDPR)

a) "Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified.

In some applications, only the internal client number, e.g. a depositary/account number is used instead of the actual name. Access to the additional information needed to identify the person is strictly controlled by Internal Access Control measures (see above) respecting the need to know principle.

b) "Anonymisation" of data means processing them with the aim of irreversibly preventing the identification of the individual to whom they relate. Data can be considered anonymised when they don't allow identification of the individuals to whom they relate, and if no individual can be identified from the data by any further processing of that data or by processing them together with other information which is available or likely to be available.

Test and production environments are logically segregated

Test data are anonymized.

1.5 Other measures on confidentiality

A directive requires that for confidential data the “print2me“ function has to be used. Repetitive checks are being carried out in order to prevent that confidential printouts are left in the printer rooms.

A clean desk policy is in place.

2 INTEGRITY (ARTICLE 32 SECTION 1 LIT. B GDPR)

2.1 Data Transfer Control

It must be ensured that personal data cannot be read, copied, changed or deleted when being transmitted electronically or during transport, or when saved to data storage media:

a) Electronic signature for E-mails is implemented
b) When using external networks for transmission of personal data, encryption methods are available e.g. TLS, HTTPS, SSH, SFTP.
c) Access to the computer systems of CBG is possible from the outside via a secure VPN connection only.
d) Physical data transmission is logged and confirmed.
e) Electronic data transmission is logged and controlled.
f) The mobile PCs feature hard disk encryption.
g) An agreement is in place with the disposal company that clearly deals with the collection, interim storage and destruction of physically stored data (e.g. paper, disk, fiche) in accordance with German DIN standard 66399.

2.2 Data Entry Control

Verification whether and by whom personal data are entered, changed or deleted in a data processing system, e.g. by logging or document version management.

a) Unique user ID is in place.

b) High privilege access rights are separated from business activities and can be linked to an identified user.

c) Admin activities are recorded.

d) Based on risk analysis, data entry is possible only with a 4-eyes-principle.

e) Access to personal data is monitored and logged in each application processing personal data.

3 AVAILABILITY AND RESILIENCE (ARTICLE 32 SECTION 1 LIT. B, C GDPR)

3.1 Availability Control (Article 32 Section 1 lit. B GDPR)

Prevention of accidental or wilful destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting procedures and contingency planning

a) CBG data recovery is structured around the backup policy that defines the standards and practices for recovery
b) Data recovery process ("DRP") and penetration tests are performed to ensure the robustness of the data processing.
c) Secured facilities against burglary, fire, flooding, heat and power emergency supply in hardware areas are in place.
d) Firewalls, intrusion detection system ("IDS"), Intrusion Prevention System ("IPS") and web application firewall ("WAF") are implemented.
e) Technical vulnerability dashboards with our IT providers are in place, review against SLA is done on a regular basis.
f) Based on risk analysis, systems and data are saved daily and maintained securely.
g) Restoration tests are performed regularly.

3.2 Rapid Recovery (Article 32 Section 1 lit. C GDPR)

a) Business Continuity Management ("BCM") procedures are in place and executed
b) Disaster recovery plan tests are executed regularly.

4 4 PROCEDURES FOR REGULAR TESTING, ASSESSMENT AND EVALUATION (ARTICLE 32 SECTION 1 LIT. D GDPR; ARTICLE 25 SECTION 1 GDPR)

4.1 Data Protection Management

Measures especially designed to keep the measures for data security described here up to date.

a) A dedicated internal control system ("ICS") process on CBG's technical and organizational measures is in place to ensure their implementation.

b) TOMs are regularly reviewed by the local CISO and Data Protection Officer ("DPO").

4.2 Incident Response Management

a) There is an incident process in place. Internally, the IT security group monitors irregularities and sets up actions against them.

b) The providers are contractually obliged to report incidents and take appropriate actions.

c) Relevant sub-processors have to use a dedicated reporting form in case of an assumed data breach.

4.3 Data Protection by Design and Default (Article 25 Section 2 GDPR)

a) A basic protection level is defined by the Information Security Policy that defines generic standard measures which have to be applied regardless of the risk analysis

b) In addition, IT systems are protected by a list of second-layer measures according to their security level identified during the risk analysis.

c) The risk analysis is reviewed regularly.

d) A project methodology procedure is in place to ensure a secure development lifecycle that provides privacy-by-design principles.

4.4 Order or contract control

There is a dedicated ICS process on outsourcing- and data protection-management to ensure the correct processing of CBG's data by its relevant providers, in accordance with the GDPR and the respective contractual obligations of the provider.