CACEIS position with regards to the General Data Processing Regulation (EU) 2016/679 (“GDPR”)

Summary of data processing performed:	CACEIS Investor services is an asset servicing bank specializing in post-trade functions related to administration and monitoring of all asset classes. With a solid IT infrastructure, we provide execution, clearing, custody, depositary and asset valuation services in markets worldwide to assist institutional and corporate clients in meeting their business development objectives. It is a regulated company and as such complies to national, European and international legal and regulatory requirements.

Table of contents

1 Overview of the data processed by CACEIS (GDPR Chapter 1 and 2)

CACEIS provides (a) a range of core market services for their institutional clients ranging from execution, clearing, trade management, position keeping, foreign exchange, custody and cash services, portfolio administration, master data services, etc; (b) tailored services for the dedicated needs of Asset managers, Institutions, Corporate Banks, Brokers and Private Equity funds. Including Trustee, fund structuring, fund distribution, general meetings, depositary and position keeping etc; (c) digital services to manage your data.

To perform and deliver these services, CACEIS not only complies with the technical standards and guidelines, but also ensures compliance with national and international banking and investments services providers regulations within the EU and elsewhere.

Information is therefore collected and processed to meet those requirements. Personal data is collected and used for legal and regulatory purposes, including for the contractual execution of the contract. Only necessary data are collected, processed and then archived to meet stipulated retention requirements. Data is never used for other purposes.

CACEIS generally considers itself to be the “data controller” of the services provided to its customers.

Personal data collected, stored and used includes:

- Data of natural persons acting as representatives of CACEIS clients and their investors
- Data of natural persons acting as representatives of CACEIS prospects
- Third parties data entrusted to us by our customers

With the exception of a few rare processing operations, CACEIS does not process any particular category (art. 9) of personal data based on regulatory obligations.

2 Upholding of the Individual Rights of the data subject (GDPR Chapter 4)

Individual “rights” of the data subject are ensured, protected and guaranteed through the implementation of CACEIS internal policies and procedures, which are governed, monitored and evaluated by the Data Protection Officer.

Personal data processed by CACEIS is either provided by clients for contractual or regulatory purposes, or collected directly by CACEIS for legal or regulatory reasons. This personal data obtained in a Business to Business relationship is used only for the purposes of meeting those agreed contractual commitments and to meet the national and international regulatory and legal constraints of financial products, markets and investments services. The personal data is therefore kept and archived for these purposes.

CACEIS do not perform profiling based on Personal data and, for the purposes such as AML and KYC Personal information may be shared with the authorities upon demand (e.g. ACPR, ECB, Data protection authorities).

All requests received by CACEIS will be processed in accordance with applicable regulations. The rights of persons whose personal data is processed and how to exercise these rights are described in the CACEIS data privacy notices, which are also available on the CACEIS website: **https://www.caceis.com/who-we-are/compliance/**

The data subject's rights include the following :

- Right to basic information
- Right of access
- Right of rectification
- Right to erasure and the "right to be forgotten"
- The right to restrict processing
- Right to object to processing

3 CACEIS' Set-up for Applying the General Data Protection Regulation

3.1 CACEIS LEGAL SET-UP

CACEIS defined the group strategy, an internal organization and group-wide procedures to implement GDPR in term of contract and legal matters towards clients, suppliers, counterparties, data subjects and intra-group.

The purpose is to define the contractual and legal setup that all CACEIS Group entities and branches shall have in place with third parties (clients, suppliers and counterparties), data subjects as well as amongst the group entities and branches regarding personal data protection in order to implement the requirements triggered by the GDPR.

3.2 QUALIFICATION OF CACEIS' ROLE UNDER GDPR

Definitions of Controller and Processor are as follows:

Data Controller or Controller	As per Art. 4 (7) of GDPR, the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**; where the purposes and means of such processing are determined by European Union or member state law, the controller or the specific criteria for its nomination may be provided for by European Union or member state law.

Data Processor or Processor	As per Art. 4 (8) of GDPR, a natural or legal person, public authority, agency or other body which processes personal data **on behalf of the Controller**

3.2.1 Qualification of CACEIS under GDPR vis-à vis its clients

When CACEIS provides services to its clients, they are rendered by CACEIS firstly, in compliance with all regulations and obligations imposed on CACEIS (including personal data retention periods); secondly, by giving its clients the benefit of industrialized services with all the necessary skills, this leads CACEIS itself to set the purposes and means of the processing carried out. Consequently CACEIS qualifies as a "Data Controller" in accordance with the European Data Protection Board ("EDPB") Guidelines 07/2020 on the concepts of controller and processor in the GDPR .

Nevertheless, should a specific processing be identified by a client as being processed by CACEIS in the capacity of Processor on behalf of the client acting in the capacity of Controller according to the criteria of the EDPB, the instructions of the client regarding such a specific processing shall be provided in writing to CACEIS in a binding document to be agreed with CACEIS and include all characteristics required as per Article 28.3 of the GDPR (subject-matter, duration,

nature and purpose of the processing, type of personal data and categories of data subjects from whom the processing of personal data is carried out by CACEIS on behalf of the client).

The table below gives examples of the characteristics of the processing carried out by CACEIS:

Services where processing might be carried out by CACEIS	Subject matter, nature and purpose of the processing	Categories of data subjects	Type of Personal Data	Legal basis for personal data processing	Duration of the processing	Classification of CACEIS	Comments
Depositary bank/ trustee (Depositary function, Asset Retention and Position Holding)	• Monitoring the regularity of investment decisions and monitoring regulatory ratios Custody of fund assets (account keeping for financial assets and position keeping for non-financial assets)	Investors	Identifiers, civil status, etc...	Contract execution	Processing will continue for the duration of the relevant service agreement, and thereafter, without the	Controller	
Custody	• Settlement processing • Corporate acting processing on lent borrowed positions or Buy/Sell positions • Tax reporting • General meeting processing	Clients, investors	Identification information, Tax information	Contract execution	Processing will continue for the duration of the relevant service agreement, and thereafter, without the personal	Controller	

Asset Administration and Accounting: Regulatory Reporting	Production of regulatory reports on behalf of clients (funds, management companies, investment managers or insurance companies) in accordance with the relevant service agreement	Investors	Depending upon the scope of the service, personal or business details (Surname, first name, email address, telephone numbers, bank account details) necessary for the performance of the service	Legitimate interest, contract execution , legal obligation	Processing will continue for the duration of the relevant service agreement, and thereafter, without the personal	Controller	CACEIS is acting for the clients but comply to regulatory or laws obligations
AML/KYC due diligence on behalf of clients, investor order processing and/or information management	Processing personal data of clients' investors in accordance the applicable AML/KYC regulations and the relevant service agreement	Investors and their beneficial owners	Name, date of birth, postal and email addresses, passport identification numbers, phone numbers, bank account numbers and financial information for source of wealth and source of funds	Legitimate interest, contract execution, legal obligation	Processing will continue for the duration of the relevant service agreement, and thereafter, without the personal	Controller	CACEIS meets there its own regulatory obligations ; these obligations are shared with the client ; neither clients nor CACEIS have the possibility to change the processing regarding KYC/AML nor the type of personal data to be collected. No documented instructions can be given by clients to CACEIS to carry on this processing.

Services related to Distribution: Transfer Agent, Paying Agent, PTA (prime transfer agent), RNI, Order routing, Dealing, Monitoring of investor orders and/or information on distribution networks If applicable, keeping locally the shareholder or unitholder register.	Processing related to local distribution and/or cross-border distribution in accordance with the relevant service agreement	Investors	Personal or business details (Surname, first name, email address, telephone numbers, bank account details) necessary for the performance of the service and possibly some special categories of personal data	Legitimate interest, contract execution, legal obligation	Processing will continue for the duration of the relevant service agreement, and thereafter, without the personal data being retained longer than necessary under applicable law.	Controller	CACEIS is acting according to laws and regulation, it is an industrial processing operation without customization
Domiciliation of funds and company secretarial services to funds : In particular, assistance provided for general meetings of shareholders and board of directors.	Registration of funds' directors' personal data in the Trade Register. Providing company secretarial assistance in respect of general meetings and board meetings, and associated secretarial services in accordance with the relevant service agreement	Fund directors, investors, and as the case might be investment managers beneficial owners	Personal or business details (Surname, first name, email address, telephone numbers, potentially bank account details)necessary for the performance of the service and possibly some special categories of personal data	Legitimate interest, contract execution, legal obligation	Processing will continue for the duration of the relevant service agreement, and thereafter, without the personal data being retained longer than	Controller	No direct documented instructions are received from the client regarding the processing of personal data or the personal data. The domiciliation team is only processing personal data according to the applicable local regulation or legitimate interest to carry on the service.

Custody Network maintenance (part of custody services)	Providing personal data of investors and beneficial owner to sub- custodians where required by local market or applicable law	Investors and their beneficial owners	Name, date of birth, postal and email addresses, passport identification numbers, phone numbers, bank account numbers and financial information for source of wealth and source of funds verification, and possibly some special	Legitimate interest to run the service, legal obligation as per applicable local law.	Processing will continue as necessary in respect of local regulation.	Controller	
Private Equity, Real Estate & Securitization : Administration of funds	Cash instructions / Register keeping/Constitute or update and control investors' KYC	Investors, third parties (tenants)	Personal or business details (Surname, first name, email address, telephone numbers, bank account details) necessary for the performance of the service	Legitimate interest, legal obligation	Processing will continue for the duration of the relevant service agreement, and thereafter, personal	Controller	
Multi-Channel communication: OLIS, OLISMOBILE, SWIFT & Other formats,TEEPI (Tailored Electronic Exchange Platform forInvestors)	Unique internet portal for all our client services ;mobility service for essential information for asset managers (VL monitoring and validation, Real- time monitoring of investors) ; multi- service connection solutions via SWIFT messaging ; data exchange network for relations between financial institutions and management companies	Investors users As the case might be directors financial institutions and management companies	Personal or business details (Surname, first name, email address, telephone numbers, bank account details) necessary for the performance of the service	Legitimate interest, contract execution for clients, legal obligation		Controller	

When outsourcing services to suppliers, the supplier generally qualifies as Data Processor of CACEIS for processing personal data in the context of the outsourced service and subject to CACEIS' instructions (whether CACEIS is controller or processor of personal data vis-à-vis a client).

CACEIS uses standard clauses for any contractual relationship with its suppliers. The purpose of the standard clause is to ensure that the supplier carries out any processing of personal data in accordance with the GDPR and to provide relevant instructions in this regard.

Some other specific situation may require further analysis of the qualification and adjustment of the contractual set-up. This is the case notably for relationships with consultants, sub-custodians and financial counterparties.

In any and all cases, a contractual arrangement shall be made between the parties to set the qualification, define the respective obligations and agree on the flow of communication or actions amongst the parties in order to comply with GDPR.

4 Organisational Security measures

4.1 Data protection officer (GDPR Chapter 4, Section 4, Articles 37, 38, 39)

CACEIS has appointed a DPO for the Group. The details are available via the Corporate internet and Intranet web sites. The DPO is a direct report of CACEIS Chief Compliance Officer, a member of the Executive Committee. The DPO will be in charge of data protection activities for the Group and coordinate a network of site level and entity level data protection correspondents.

The CACEIS DPO can be reached via email: caceisdpo@caceis.com

4.2 Commitment to data secrecy and confidentiality (GDPR Chapter 4, Section 2, Article 32.1)

All CACEIS employees are committed to data, banking, business secrecy and confidentiality. This, within the scope and bounds of national employment laws (e.g. contractual, corporate charter, commitment letters, ...). This commitment includes an obligation to confidentiality after the termination or change of contract of employment.

CACEIS Information Security passport is a guideline issued to employees to outline best practices that are used in performing their business activities. It is fully aligned with Crédit Agricole's procedures and best practices.

4.3 Work directives, coaching and training sessions on data protection (GDPR Chapter 4, Section 4, Article 39.1(b))

CACEIS publishes and maintains policies and guidelines for **privacy** and **protection of personal data**. The CACEIS Group Data Protection and Information Security policy requires all entities to ensure compliance with their national and international legal requirements. In addition, CACEIS has published a specific HR Charter for the protection of employee personally identifiable information (PII).

To ensure continued Employee development and awareness, we make use of industry standard training platforms for the delivery of up-to-date content to enable staff to self-manage their development throughout their career. Awareness campaigns for regulatory and industry practices, are delivered to CACEIS employees either via workshop meetings, Q&A sessions and desktop technologies.

Registration of training and participation in the training classes is managed and tracked by HR.

4.4 Records of processing activities (GDPR Chapter 4, Section 1, Article 30)

CACEIS maintains a register of Personal Data processing operations within the meaning of Article 30 of the RGPD.

Internal procedures, processes and policies (including project governance, the collection of agreements for the launch of new products or the modification of existing products, the obligation to conduct risk studies for any new data processing or substantial modification of data processing), a mandatory annual review of the register of processing operations, ensure that CACEIS has an exhaustive and up-to-date register.

For each processing operation, the register contains the following information:

- The entity and data controller,
- Any external service providers,
- The list of personal data processed,
- Identify transfers of personal data outside CACEIS (to the Crédit Agricole Group / outside the Crédit Agricole Group, within the EU),
- Identify, when they exist, the transfers of personal information outside the EU and the way in which these transfers are secured,
- The main data protection measures.

The DPO supervises the Register of Processing and compliance with regulations. The controller and its representatives are responsible for ensuring that the information in the Register is correct and kept up to date..

4.5 Personal data breach procedures (GDPR Section 2, Article 33 and 34)

CACEIS takes all data breaches seriously, whatever their nature. The risk of personal data breaches is reviewed and appropriate measures are taken to mitigate these risks. Data breaches are managed on the basis of internal policies and guidelines associated with crisis management.

Under the direction of the CACEIS DPO, relevant documentation (policy, guidelines) has been updated in coordination with the Crédit Agricole Group. Group guidelines have been issued and incorporated.

By default, after detection, if the seriousness and scope of the incident concerning Personal Data justifies it, the CACEIS DPO, the CACEIS CISO and the Crédit Agricole Group DPO intervene in order to assess and coordinate the management of the incident and the appropriate responses. The action plan will naturally be escalated and notified to the DPOs of all affected parties if necessary and in accordance with agreed contractual arrangements.

Depending on the seriousness of the impact on the rights and freedoms of natural persons, and in accordance with article 33 of the RGPD, the CACEIS DPO will notify the Data Protection Authority (DPA) on which the CACEIS group depends and, if necessary, will inform the persons concerned. Unless, of course, the contract signed with its clients indicates that CACEIS is acting as a "processor", in which case CACEIS will not directly notify the data subjects, who remain under the responsibility of the client as the "controller" (article 34 of the RGPD).

CACEIS expects and has taken steps to ensure that processors notify CACEIS of any personal data breach within a predefined period and without undue delay.

4.6 Information Security guidelines (Chapter 2, Article 6 ; Chapter 4, Section 2, Articles 24, 25 ; and Section 3, Article 35)

Information and IT security is governed by the CACEIS Information Security Policy (a version is available on the CACEIS Internet site) and supported by specific subject matter guidelines and standard operating procedures (SOP). These cover the principal themes such as classification, roles and responsibilities, identity management and access control, infrastructure security, user technologies including desktops and mobile systems, development guidelines, data backups, etc ... These are regularly reviewed and updated to cater for emerging technologies and risks.

CACEIS Information Security passport is a guideline issued to all employees that outlines the best practices to be used in performing their business duties. It is fully aligned with Crédit Agricole’s procedures and best practices.

Risk assessments are performed for all new processing requirements and changes to existing processing. TUNES, the CACEIS risk assessment method is mandatory for all new personal data processing to comply with the obligations of "privacy by design" and "privacy by default" defined by GDPR Where the type of processing activities presents high risks to the rights and freedoms of natural persons then a Data Protection Impact Assessment (DPIA) is performed (Article 35 of the GDPR). The DPIA methodology is fully aligned to Crédit Agricole’s.

CACEIS systems are designed and embed protection measures by default and by design, these measures include some of those described above. By default, there is no access. In accordance with article 25 of the GDPR, some of the existing security guidelines will be enhanced to further reduce risks to the rights and freedoms of natural persons, in particular for special categories of data.

With regards to the development of software and systems, a specific policy addresses Acquisition, Development and Maintenance and covers topics:

- integration of security in projects
- risk analysis and security requirements

- design and implement security solution
- testing, acceptance and commissioning
- documentation
- maintenance
- integration of security in development

In addition, various procedures and standards are in place, of which:

- MESARI is used for risk assessments.
- SECAPI is a CASA group standard, which provides secure privacy-by-design principles.
- SOPs (Standard Operating Procedure) are in place in the IT department.

Software development, implementation and maintenance is documented and ensures operational procedures are maintained. The documentation uses industry best practices and standards such as COBIT and ITIL.

4.7 Data storage / processing outside Europe (GDPR Chapter 5, Article 44)

All personal data is stored and processed within the CACEIS datacentres in Europe. For some activities, that concerns principally fund administration and accounting, a small amount of remote processing takes place from CACEIS offices in either Hong-Kong or Canada.

Certain processing activities leverage third-parties, such as software development and maintenance. The activity is performed remotely on systems in European datacentres and makes use of anonymised data.

5 Technical security measures to protect Personal Data

5.1 Overview of the technical architecture

CACEIS Information Technology services are focused primarily on design, build and run of the highly automated business information systems. The systems leverage technologies such as Mainframe, Microsoft Windows, Linux, Oracle databases and Web based middleware.

The hosting of the technical platform and lights-out operational management are outsourced to DXC and located in Luxembourg. Desktop services are managed and delivered by Credit Agricole CAGIP and located in France.

5.2 Measures to pseudonymise and anonymise personal data (GDPR Chapter 4, Section 2, Article 32.1(a))

CACEIS Information Security Policy mandates that no production data is available in non-production environments (development, test, etc) unless fully anonymised. This rule applies to Personal Data.

5.3 Measures to encrypt personal data (GDPR Chapter 4, Section 2, Article 32.1(a))

Following measures are in place:

1. Mobile computers are equipped with hard disk encryption technologies
2. TLS security protocol has been implemented for email exchange
3. HTTPS security protocol is used to secure access to web-based applications
4. Data transfers with clients are encrypted
5. A solution is available to encrypt sensitive emails

5.4 Measures to ensure ongoing confidentiality (GDPR Chapter 4, Section 2, Article 32.1(b))

Following measures are in place:

1. Buildings and external areas are controlled by security personnel. Alarms are in place. Entrances are protected by technical access controls (entrance control and video control) and organizational measures (front desk)
2. Proper identification and review of users and administrators accessing personal data
3. Password policy implemented
4. Screen lockout after inactivity period
5. Secure network infrastructure
6. The USB are blocked by default
7. Access to personal data by unauthorised individuals is prevented
8. Secured physical transportation
9. Disposal of used PCs data storage media and written matter is controlled
10. Secure printing solution is deployed

5.5 Measures to ensure ongoing data integrity (GDPR Chapter 4, Section 2, Article 32.1(b))

Following measures are in place:

1. Unique user ID is in place
2. High privilege access rights and separated from business activities and can be link to an identified user
3. Physical data transmission is logged and confirmed
4. Electronic data transmission is logged and controlled
5. Based on risk analysis, data entry for certain high-risk applications is possible only with a 4-eyes-principle.
6. Access to personal data is monitored and logged
7. Administration activities are recorded

5.6 Measures to ensure ongoing availability (GDPR Chapter 4, Section 2, Article 32.1(b) (c))

Following measures are in place:

1. SLA are in place with providers
2. Secured facilities against burglary, fire, flooding, heat and power failures
3. Data backup centres and procedures are in place to restore the availability of personal data in a timely manner
4. Recovery/restoration are tested
5. BCM (Business continuity plan) concepts have been designed and implemented.
6. Specific high-risk scenarios have been developed to cover incidents such as people related (virus, flooding, …) and technology related (massive desktop outage, logical failure of datacentres technology caused by human error, technology failure or cyber threats).
7. Regular testing of BCP and DRP plans to ensure the systems and processes are fully operational and up to date.

5.7 Measures to ensure ongoing resilience of the systems and services (GDPR Chapter 4, Section 2, Article 32.1(b))

Following measures are in place:

1. Each application is subject to risk assessments that map the appropriate security controls and security measures (C.I.A). Application software is subject to internal SECAPI architecture and development standard, is maintained, tested and reviewed prior to Change Control permitting promotion to production environments.
2. DRP and Penetration test are performed to ensure the robustness of the data processing environment.
3. Regular security scans of the network that identifies the equipment attached, the software in use and any vulnerability. Remediation plans are elaborated for identified high-priority items.
4. Threat intelligence solution is used to evaluate and analyse the risk levels.
5. Secured facilities against theft, fire, flooding, heat and power emergency supply in hardware areas.
6. Data backup procedures are in place to restore the availability of personal data in a timely manner.
7. Recovery/restoration are tested.

5.8 Measures for regular reviewing, assessing and evaluating of the effectiveness of technical and organisational measures

(GDPR Chapter 4, Section 2, Article 32.1(d))

Following measures are in place:

1. Internal controls have been designed and implemented to monitor the efficiency and effectiveness. These include operational level controls (Level 1), consolidated controls (level 2 and 2.1) and Level 3 controls.
2. Audits are performed internally and externally,
3. Regular testing of disaster recovery and business continuity plans
4. The RGPD control plan is implemented with monthly and quarterly reporting.
5. Technical and Organizational Measures (TOMs) are regularly reviewed.

6 Detail for specific technical and organisational protection measures

6.1 Physical security measures

6.1.1 CACEIS Office space

CACEIS Buildings and office space are protected 24/7 using technologies such as video surveillance, intrusion detection, and nightly rounds of security staff.

Entry into building requires prior authorisation and an access pass. The badges provide restricted access and circulation within the buildings. All employees are issued with a badge. Visitors are issued with a temporary access pass once their identity has been confirmed and the visit authorised by a CACEIS employee.

6.1.2 Data centre processing facilities

CACEIS processing facilities are very tightly controlled. CACEIS maintains formal access procedures for allowing physical access to the data centres. The data centres are housed in facilities that require specific electronic card key access and proof of identity. Access lists are maintained and reviewed frequently. CACEIS's data centres require on-site security operations responsible for monitoring and logging all physical data centre security functions 24 hours a day, 7 days a week.

6.2 Authentication management and control

6.2.1 User Identification

Policies and procedures are defined to ensure that proper identification of users and administrators accessing personal data are identified.

CACEIS employs a centralized identity and access management system (IAM). This system is responsible for the allocation of user identities, the user identities are unique for all personnel that wish to access and use any part of the CACEIS Information System. Access can only occur via a CACEIS network connected workstation. These require a personal user identity and at a minimum a password. In some instances, specific applications may require two factor identification.

CACES Information Security Policies mandates that privileges should be segregated and distinct from regular business activities, therefore a dedicated user ID is provisioned to those nominated individuals. Privileges include special system and application administration tasks.

To ensure the USER ID remain relevant, recertification and conciliation campaigns are regularly performed. Thus, any orphans and invalid USER IDs are immediately disabled and removed as necessary (e.g. timely deactivation of USER IDs of employees that have left the company).

6.2.2 Authentication

The IAM controls access to production systems based on defined rules. CACEIS leverages technologies such as LDAP, Kerberos and a proprietary system utilizing RSA keys (or others logical keys) to provide secure and flexible authentication mechanisms. These mechanisms are designed to grant only approved access rights. Authentication to technical systems is additionally controlled via a dedicated platform.

Authentication with CACIS generally requires a personal secret password, although in a few instances, two factor authentication is performed using chip cards and token devices. The password management rules and standards are governed by the Information Security Policies. These standards include such restrictions as password reuse, password strength and password lifetime. The following password rules are implemented and controlled within the windows active directory:

- At least 12 characters is defined in the policy
- Maximum password lifetime: 90 days
- Locked account: after 5 login attempts

6.2.3 Access to data processing systems

All data processing systems (desktops, servers, ..) are connected by an internal CACEIS network. Access is data processing systems is only possible from the CACEIS network.

The CACEIS network design standards are based on the Crédit Agricole standards which are always at the best standards of the market. CACEIS network is physically and logically segregated (purpose, risk, technology) integrating security technology that monitors, detects and prevents intrusion (Firewalls, IDS,

IPS and WAF). System redundancy and fault tolerance is part of the network architecture to ensure access to data processing systems complies with Business SLAs requirements.

System settings follow a "default-deny" principle. Meaning that firewall and router configurations have been set up in order to restrict the traffic inbound and outbound and that everything not explicitly allowed is prohibited. By default, and by design these settings deny all flows and communication across boundaries, only those flows defined are authorised. A Change Acceptance Board (CAB) is dedicated to network flows, protocols and services. Controls are implemented to monitor the compliance with our technical policies.

Monitoring is performed in real-time by the Credit Agricole CERT monitor 24x7 and CACEIS SOC. In the event of warning or irregularities the Information Technology Security Officer (ITSO) and SOC initiate responses according to agreed procedures.

6.3 Access control by authorisation management

Access assignment is formalized and governed by the CACEIS Access Control Policy (part of the Information Security Policies). The Standard operating procedure (SOP) describes how the management process operates, including the authorisation and attribution of “Access”.

Access is allowed on a need to know basis only. Access authorisation is performed using workflow and is required by both the manager and the application owner, in some instances additional approval may be required. The assignment of specific rights is handled by the application and attributed once authorised by managers.

The authorisation management workflows are performed within the IAM system, where the provision and the attribution of rights is managed using pre-defined business profiles. Only the Business profile manager can apply for a change Business profiles. The approval from the business profile manager, the business application owner and the risk department are required to assign new access to a Business Profile.

The IAM system performs revocation automatically. Complementary to this, recertification campaigns are performed regularly by the manager and the application owner to certify the need is still appropriate.

The business profiles, and associated access entitlements, are defined to enforce the principles of “need to know”, “least privilege”, and “segregation of duties”. Reviews are performed with the risk department to check toxic access right combinations.

6.4 Copy Protection of data

The Information Security Policy of CACEIS defines rules how to use media and to handle data. Use of portable digital media is not permitted. USB ports are blocked by default and individuals may request temporary activation under strict conditions. Only external media approved by CACEIS can be used to store data.

6.5 Disclosure Control

6.5.1 Information transport and Electronic data transmission

The Information Security Policies and SOPs define secure transportation measures for the protection against unauthorized access and misuse.

Physical transportation of information, in particular confidential and sensitive information, is restricted. CACEIS make use of specific secure transport services.

Electronic Transfers, CACEIS transfers the majority of information electronically, via secured internet connections and secure file transfer. Each sender participating in the transmission is identified using electronic signatures. Data transmission of personal data across external networks uses strong cryptography and secure protocols, such as the use of TLS, SSH, HTTPS, SFTP, IPSEC. All electronic data transmissions are logged and monitored.

Security measures are implemented to monitor and control the flow of data through endpoints and external networks. Such measures include Firewalls, IDS, IPS and WAF technologies. A Change Acceptance Board is dedicated to network flows, protocols and services reviews and plans requests.

6.5.2 Data Security

CACEIS Information Security Policies and SOPs define our approach for asset classification including application assets and data assets. A majority of assets are inventoried and classified based on risk assessments that include the evaluation of Information Security axioms Confidentiality, Integrity, Availability. This approach includes the classification of Personally Data. The asset classification process is a defining step to ensure that the choice of security measures and controls is performed according to the level of criticality of the asset.

6.5.3 System resilience and penetration tests

Both system resilience and robustness are important aspects of the services delivered by CACEIS. To ensure these meet with our Business standards we schedule and perform numerous data processing tests throughout the year. These tests include Business Continuity (BCM) and Disaster Recovery Tests (DRP), and Penetration tests (PEN TEST). Change control is part of the process that contributes by ensuring testing is properly performed prior to delivery of changes into production environments.

DRP includes ensuring plans are documented, up-to-date and tested for a number of defined disaster scenarios. Data recovery includes our ability to restore information. Guided by the Backup Policy that defines the standards and practices for secure information backup and recovery, we perform regular restoration tests.

PEN TESTS are performed regularly by CACEIS on our critical infrastructure to test the strength, robustness, resilience, performance and maintain water tightness of the security systems measures deployed. In addition, CACEIS has a threat intelligence tool that constantly analyzes the state of its system and network to detect potential security breaches.

6.5.4 Portable PCs (laptops) and mobile devices

Protection measures for Portable PCs (laptops) and mobile devices are defined by the Information Security Policy and described in the Information Security standards and SOPs. The use of mobile devices (laptops, smartphones, tablets, etc.) is subject to particular rules. Users agree to respect these rules by signing a specific document when issued with the device in question.

Information on laptops is protected by hard disk encryption technologies and by others security measures managed by MDM (Mobile Device Management) solution. In case of loss or theft, the data stored on the mobile devices can be erased remotely by CACEIS.

6.5.5 Disposal of used PCs and data storage media

CACEIS has defined and implemented appropriate procedures (SOP) for the secured transportation and disposal of ICT assets, with data storage media subject to destruction standard EN 66399. CACEIS has also defined and implemented appropriate procedures (SOP) for the secure erasure of data from storage media.

6.6 Availability control

6.6.1 Security facilities in hardware areas (server rooms, data centre)

Information systems are hosted within Tier IV data centers that meet highest level of protection and security requirements. The Tier IV data centers are protected against power interruption, power loss and they are both located in areas that are not subject to flooding and seismic activity. To meet the exacting criteria, both power and telecoms are secured via numerous entries.

6.6.2 Data backup

Management of data backup and recovery is performed as follows:

- SOPs have been developed to ensure the backup and recovery of systems in line with predefined business requirements.
- Backups are performed daily and mirrored to the secondary site.
- Backup and recovery procedures are tested at least yearly to ensure they are fully operational and maintained up-to-date.

6.6.3 Precautions against disasters

CACEIS supports a number of pre-defined Credit Agricole major crisis scenarios and has implemented SOPs to respond to these in the event of a disaster.

With regards to our data centers, they are fault-tolerant, and independently capable of resorbing an outage of its partner data centers and ensuring the continuity of service delivery. Our crises management plans ensure failover management.

CACEIS performs several tests per year to ensure that the technical and organizational measures in case of disaster, are operational. These tests are carried out under the control of the business line which validates the result of the tests.

6.7 Audit trail for personal data input, changes and erasures

Access to data (inputs, changes, erasures) using corporate applications is logged by applications themselves, the applications have some monitoring solution carried out by business.

Individual users accessing personal data is also logged and monitored. This means that instances of access to personal data stored in applications is monitored and logged (read, write, update, ..).

Administration activities (e.g. recording log-on attempts, exceptions, faults, etc.) are fully logged with event logs regularly reviewed. Dedicated actions are implemented where suitable to mitigate any process related risk. The controlling takes the result of the monitoring and performs corrective actions to remediate any specific breach of Corporate rules. CACEIS IT Security Officer is responsible to initiate the dedicated process.

For the control of unstructured data, CACEIS relies on the Varonis solution to control access rights to shared directories and access to these data.

6.8 Data deletion and restriction of processing

CACEIS data retention policy is to maintain data no longer than legally, regulatory or contractually required.

6.9 Sub-Contracting control

Services corresponding to predefined criteria are closely monitored according to the predefined Credit Agricole Guidelines for Outsourced Essential services (OES) (PSEE in French). These are complemented by a specific CACEIS IT outsourcing policy based on ISO 37500. All sub-contractors are subject to the CACEIS clauses of confidentiality and CACEIS Information Security Policy.

All sub-contractors are evaluated annually on the basis of a compliance questionnaire or, in some cases, by audits.