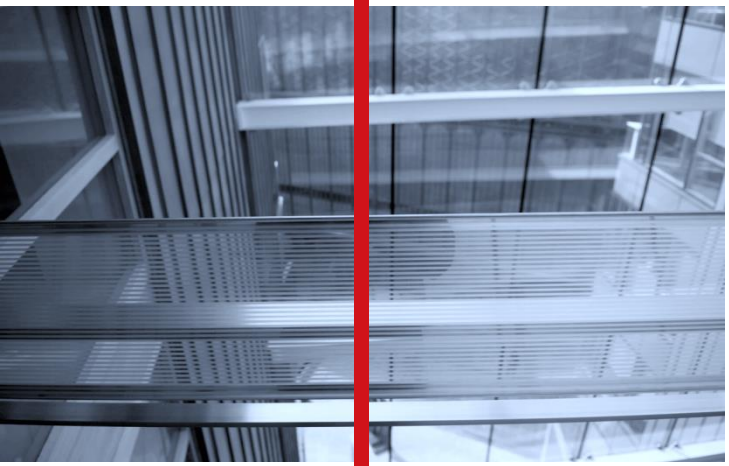
IMPLEMENTATION OF THE GENERAL DATA PROTCETION REGULATION (GDPR)

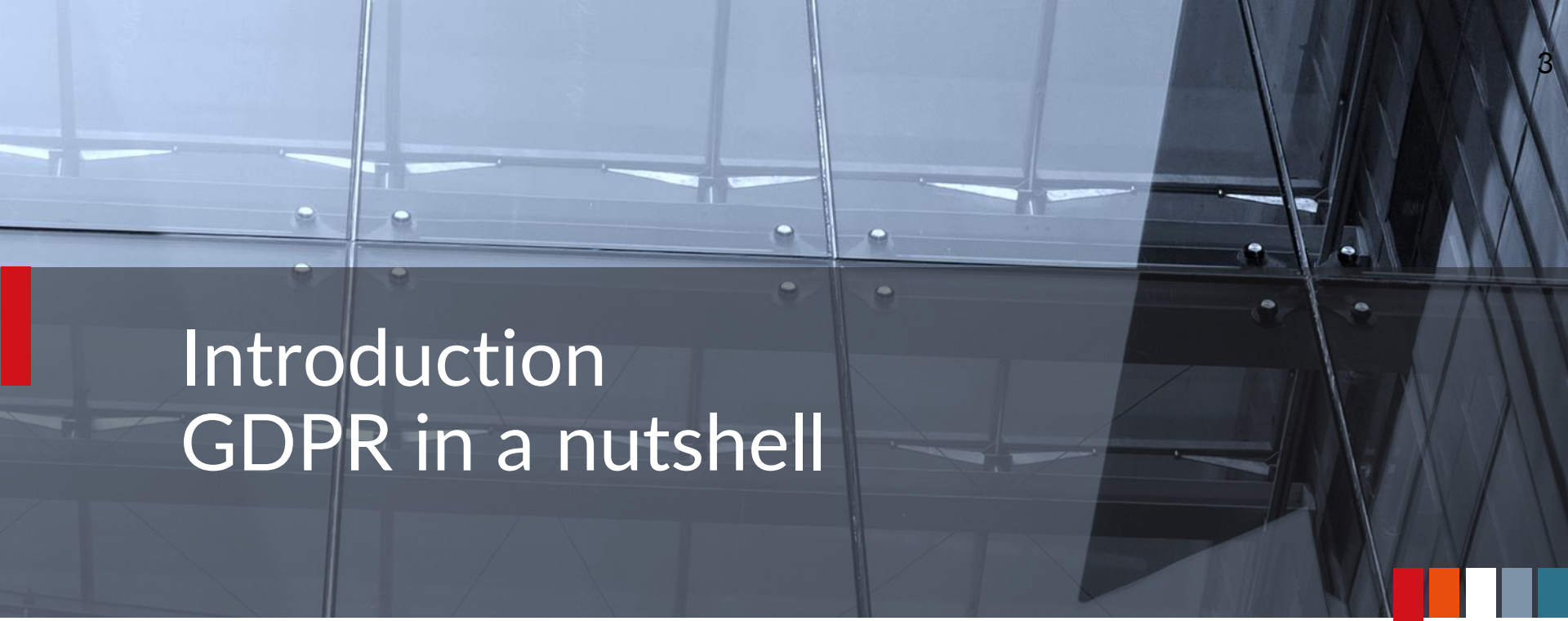
May, 2018

caceis
INVESTOR SERVICES

Agenda



1. Introduction : GDPR in a nutshell
2. Main impacts for CACEIS Group
3. A new governance and adapted procedures
4. Protecting personal data
5. Updated relationships with third parties



Introduction
GDPR in a nutshell

GDPR IN A NUTSHELL

- The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy

- All companies or institutions, whatever their business, maintaining or processing personal data of European citizens, are in the scope

- GDPR will come into force on May 25th, 2018

GDPR KEY POINTS

REINFORCEMENT OF DATA SUBJECTS RIGTHS

GDPR is enhancing existing rights and introducing a new right to data portability

RESPONSABILISATION OF THE ACTORS

Accountability is a recurring theme of GDPR, Organisations need to be able to prove that they have done the right thing to regulators, to data subjects and potentially to shareholders and the media

HARMONISATION & COOPERATION

As GDPR will become law without the need for any secondary implementing laws, there will be a greater degree of harmonisation across Europe relative to the current regime

TOUGHER SANCTIONS

GDPR joins anti-bribery and anti-trust laws as having some of the very highest sanctions for non-compliance including revenue based fines of up to 20 M€ or 4% of annual worldwide turnover

GDPR KEY POINTS

Which data is subject to the GDPR ?

- **Personal data (that can be linked to an identified or identifiable living physical person) such as:**
  - Identifiers, civil status, identity, photos, …
  - Personal life
  - Professional life
  - Financial information
  - Connection identifiers (IP address, logs, etc.)
  - Localization information (GPS Data, GSM, etc

Personal data, tagged as sensitive » (article 9 special categories of personal data)

- **The collecting and processing of sensitive personal data is not allowed.**

  Nonetheless, to the extent that the purpose of the processing activity requires it, then an exception may be granted if:

  - The person has given their express consent for the processing activity;
  - The processing activity is justified by a public interest and has been authorised by the DPA or a National State law;
  - The collection and processing of the data must by motivated on a case by case basis with regard to the sought objectives.

- Types of sensitive personal data

  - Data revealing racial or ethnic origin
  - Data revealing political opinion
  - Data revealing religion or beliefs
  - Data revealing trade union membership
  - Genetic data
  - Biometric data for unique identification
  - Health status
  - Data revealing the personal sex life or sexual orientation
  - Data revealing criminal records or penalties

Main impacts for CACEIS Group

Main impacts for CACEIS

- As a major player in the Asset Servicing business (custodian bank, trustee, fund administrator….) CACEIS has a vast experience of the implementation of any kind of new regulation and, will as per usual, be ready.

- CACEIS has performed a thorough analysis of all our businesses and processes with regards to the GDPR :
  - CACEIS deals mostly with eligible counterparties and professional clients
  - CACEIS only collects personal data from clients when required by law or when deemed necessary for rendering the service. Personal data are never used for commercial purposes, marketing or profiling.
  - On top of data of our own staff, only a few areas of our business are impacted : KYC processing, list of operational contacts at our clients, funds and corporate registers.

MAIN IMPACTS FOR CACEIS

Records of Processing Activities

- ✓ Building and maintaining the record of processing activities
- ✓ Analysis of the sensitivity of the data

Organisation of the DPO Function

- ✓ Appointment of a CACEIS Group DPO
- ✓ A network of correspondents in all the entities

Security Measures and Notification

- ✓ Complete security measures for personal data whenever required
- ✓ Update crisis management procedure in the event of a data breach of PII

Management of Rights

- ✓ Archiving rules review
- ✓ New process to manage personal rights
- ✓ Information : update of legal references on our web sites

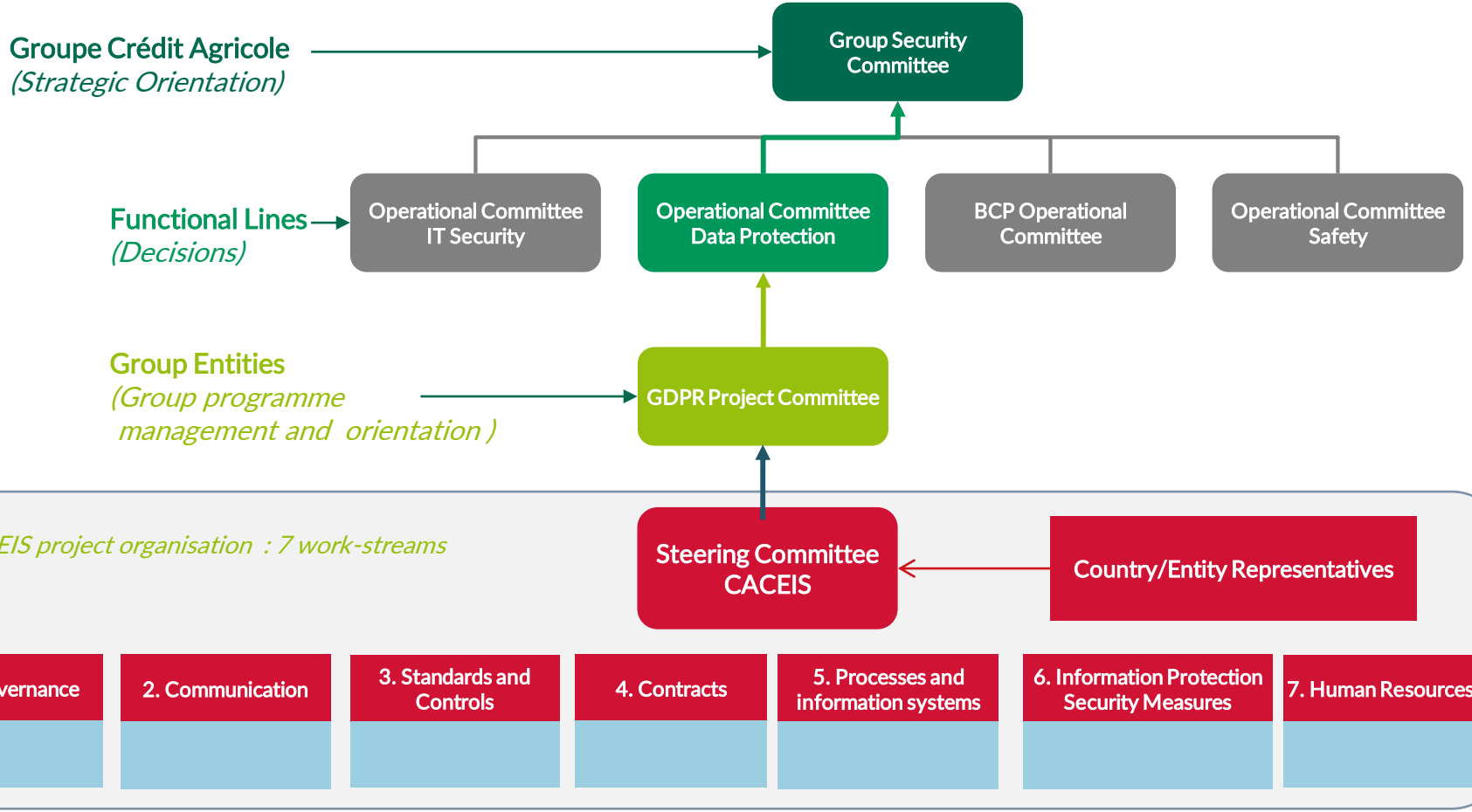
Contracts

- ✓ Clients: additional clauses or new “terms & conditions”.
- ✓ Vendors: CA Group standard additional clauses for all external providers

Training and Communication

- ✓ Group employees
- ✓ Clients

GDPR PROJECT ORGANISATION



A new governance and adapted procedures

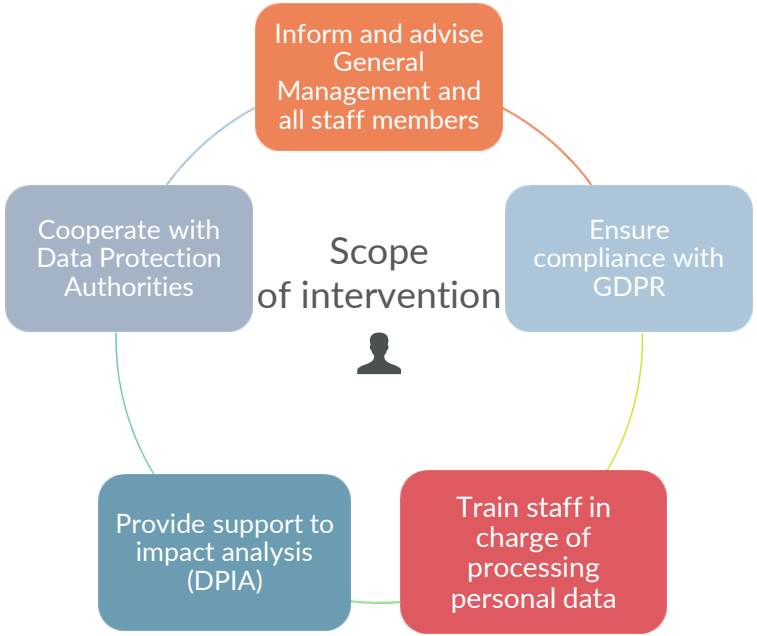
Appointment of the Data Protection Officer (DPO)

- DPO appointed at CACEIS Group level working with local correspondents in each entity
- Direct report to Exco member
- A member of Crédit Agricole Group network of DPOs
- Contact : DPOCACEIS@caceis.com

Appointment of the Data Protection Officer (DPO)

DPO's skills and role

- **Expert** : the DPO combines legal knowledge and practical skills regarding data protection solutions
- **Independant** : the DPO does not define the objective nor takes part in the processing of PII
- **Internal contact** : the DPO works in close cooperation with Exco and all involved business lines
- **External contact** : the DPO is the entry point for our clients, providers and the DPAs of markets where we operate



Setting up new standards and procedures

- **New standards :** the **DPIA** (Data Protection Impact Analysis) will complement CACEIS existing procedures for the assessment of risk in new applications development (MESARI) and its catalog of risk reduction measures :
  - « Security By Design », will guarantee from inception and for each utilization of an application, even if not initially foreseen, the highest protection of personal data;
  - « Security By default », will ensure persons concerned that only necessary personal data are used.
- **New processes to manage requests by employees or third parties (clients)** :
  - « Right to basic information» et «Right of access »
  - « Right of rectification », « Right to erasure »
  - « Right to restrict processing »,
  - « Right of data portability »
  - « Right to object to processing »,
- **New controls** :
  - For the evaluation of our providers
  - An updated Permanent Controls plan (level 1 and 2.2c)
  - An audit plan defined by the DPO

➔ **Demonstrate CACEIS ability to protect Personal Data at any time**

Protecting Personal Data

A comprehensive inventory of all Personal Data

- The Record of processing activities
  - Inventory of all processes dealing with Personal Data
  - For each process, identification of the person in charge and of possible external providers
  - Inventory of all Personal Data used
  - Recap of possible transfers of Personal Data (Group CA /out of Group CA, within EU/ out of EU…)
  - Risk assessment and related security measures

- To date
  - CACEIS listed more than 1000 applications, out of which **418** are using Personal Data (for **344,** only names and surnames of natural persons)
  - A very limited number of processes deal with special categories of personal data

Implementing protection measures

The protection measures will be derived from successive analysis made by the NAP process, MESARI and, when needed the DPIA. They will comprise:

- **Standard protection measures :**
  - Encrypt the data on hard disks, file servers , databases, … and the data flows and emails
  - « Anonymise » data in non-production environments and used for user acceptance testing or technical testing
  - Strengthen the policies concerning the use of USB devices, private webmail
  - Reinforce the management and the control of business profiles
  - Reinforce the controls on the permissions given to the IT teams
  - Deploy systems to detect the theft of data
  - Reinforce the protection of desktops and mobile devices
- **Additional measures according to the sensitivity of data :**
  - Encryption of special categories of personal data in data bases or in desktop files
  - Automatic controls to detect the presence of non-protected Personal Data
  - Obligation to encrypt emails
  - Deploy systems to detection data theft (DLP solution) to complement the existing detection mechanisms (SOC)
  - Isolate the Personal Data within network segments protected by high-level filtering solutions

Crisis management

- Update of crisis management procedures in order to take into account « Data Incident and Breach Notification Management »
  - Convening of crisis management meeting with all stakeholders of IT security management and the Group DPO
  - Diagnosis of root causes and impact of the incident
  - Remediation plan
  - Safeguarding of elements of proof (Forensic) in case of external attack or malware
  - Communication to possible 3rd parties concerned and to national DPAs (*DPA : Data Protection Authorities*) within 72 hours

Updated relationships with third parties

Revised set up with :

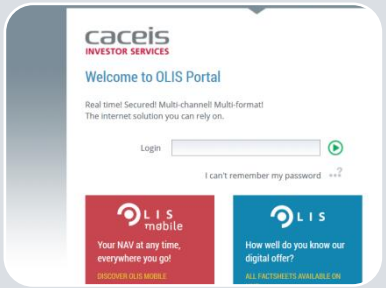
Our providers

- Full inventory of 3 rd parties handling Personal Data
- Contractual framework is complemented by new GDPR provisions defined by CA Group

Our customers

- « General terms and conditions relating to the protection of Personal Data » are issued to all our clients supplementing existing provisions
- A new template in compliance with GDPR will be incorporated to all new legal agreements
- An extract of our Records of processing activities will be made available

Regular updates via :



Caceis Flash news

Our website caceis.com

Olis portal


caceis
INVESTOR SERVICES
Solid & Innovative