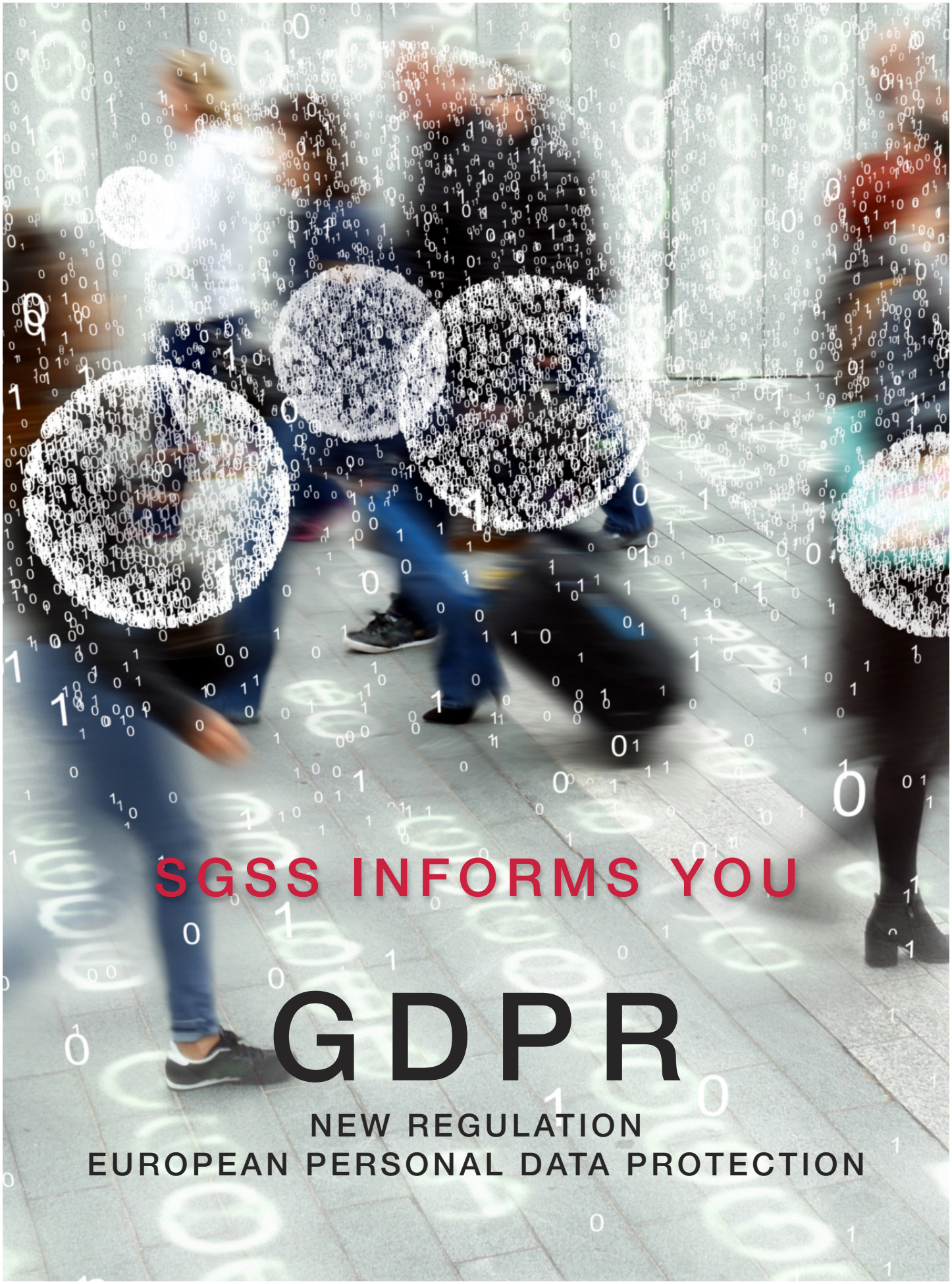

SOCIETE GENERALE
Securities Services

BUILDING TEAM SPIRIT
TOGETHER

THIS AFFECTS YOU

The amount of data generated worldwide has exploded with the digital revolution, and personal data is being increasingly used in all sectors. In light of this, and in response to concerns expressed by European citizens, the European Union, with the backing of supervisory authorities, has published the General Data Protection Regulation (GDPR). Adopted on 27 April 2016, this European regulation will enter into force on 25 May 2018.

DEFINITION OF PERSONAL DATA

Personal data is “any information relating to an identified or identifiable natural person (...), directly or indirectly, by reference to an identifier (name, identification number) or to one or more factors specific to the physical, (...), economic, (...) or social identity of that natural person”*
This may be client data, but also the data of employees, service providers, partners, shareholders, etc.

* Excerpt from Article 4 of the GDPR

General Data Protection Regulation

WHAT ARE THE OBJECTIVES OF THE GDPR?

The GDPR **strengthens existing legislation** (Directive 95/46/EC) **protecting individuals** and their **personal data,** and also aims to **protect their digital identity.** The goal is also to **harmonise data protection rules across all European countries.**

THE 3 OBJECTIVES OF THE GDPR IN DETAIL

- **Strengthen the rights of individuals and the control they have over their personal data**
  - Express **consent** is required to use information in a manner not provided for in the contract
  - Information on how clients' data is used is **transparent** and their **right to access and rectify** this information is upheld
  - **Right to be forgotten** is extended to online data
  - **Right to data portability** allows individuals to retrieve personal data to reuse or transmit it to third parties
  - Special **protection for minors**

- **Increase the accountability of persons handling data**
  - Appointment of a **controller** to maintain a **record of processing activities**
  - Appointment of a **data protection officer (DPO)**
  - Application of **privacy by design,** which seeks to minimise the data collected, limit its use to the intended purpose, and ensure that it is deleted when the legal retention period expires
  - Execution of **impact studies on privacy**
  - **In the event of leaks or personal data breaches,** notification of the supervisory authority and (where necessary) the owner of the data within 72 hours
  - Strict control of **sub-contracting activities** to guarantee compliance throughout the chain of operations

- **Enforce the regulation** under the authority of the European Data Protection Board, with enhanced cooperation between the data protection authorities and a one-stop-shop in the country of residence for cross-border operations (CNIL in France), as well as tougher penalties.

General Data Protection Regulation

WHO IS AFFECTED BY THE GDPR?

The **GDPR** applies to **all companies,** whatever their size or sector, or wherever they are registered, that collect, store and process the **personal data** of **EU residents and nationals.**

PENALTIES

The GDPR imposes **administrative fines** of up to **EUR 20 million** or **4% of turnover** in the case of a serious breach of the fundamental principles of the regulation.

Please note that with the entry into force of certain provisions of the French Digital Republic Law (the Lemaire Law) in October 2016, the maximum amount of such fines (previously set at EUR 150,000) was increased to EUR 3 million.

General Data Protection Regulation

HOW SHOULD COMPANIES PROCEED?

The first step is to conduct a **full review of processing activities** for personal data. Knowing which data is concerned, where it is stored, who uses it and who can access it will enable a proper assessment of how the GDPR will affect your company. Creating a **record of processing activities** will help you achieve this.

Next, **define a course of action:** appoint a **data protection officer (DPO), review processes,** upgrade **IT tools,** perform a **security audit,** strengthen **controls,** review **relations with sub-contractors,** organise employee **training,** etc.

These actions will require input from various departments, so begin now to make sure you are ready before May 2018.

For companies affected by the GDPR, it is now more important than ever to be vigilant and careful when processing personal data. Beyond the legal obligation to comply, a company's image and reputation among its clients are also at stake.

To find out more, visit **https://www.cnil.fr/se-preparer-au-reglement-europeen**
http://www.eugdpr.org/