Compliance:
GDPR and sensitive financial data

Ludovic Van Egroo studies how to apply GDPR to financial data in accordance with previous regulations

LUDOVIC VAN EGROO
Institut d'Etudes Politiques,
Lille, France

> COMPANIES HAVE BEEN GIVEN TWO YEARS TO IDENTIFY THEIR PERSONAL DATA USES AND IMPLEMENT MEASURES TO ENSURE THEIR PROTECTION

Digital transformation impacts all business sectors and offers many opportunities for the use of data collection. The General Data Protection Regulation (GDPR) was thus implemented to provide a regulatory and legal framework for the protection of personal data against the different ways in which it may be used.

GDPR is particularly focused on a European citizen's personal data, qualified as sensitive when the latter concerns members of an association or a political, religious, philosophical, political or trade union organisation.

Companies that have not implemented the regulatory and organisational processes related to GDPR are liable to a fine up to €20 million or 4% of their global annual revenue. Organisations are required to provide evidence of their compliance with the risk of being convicted.

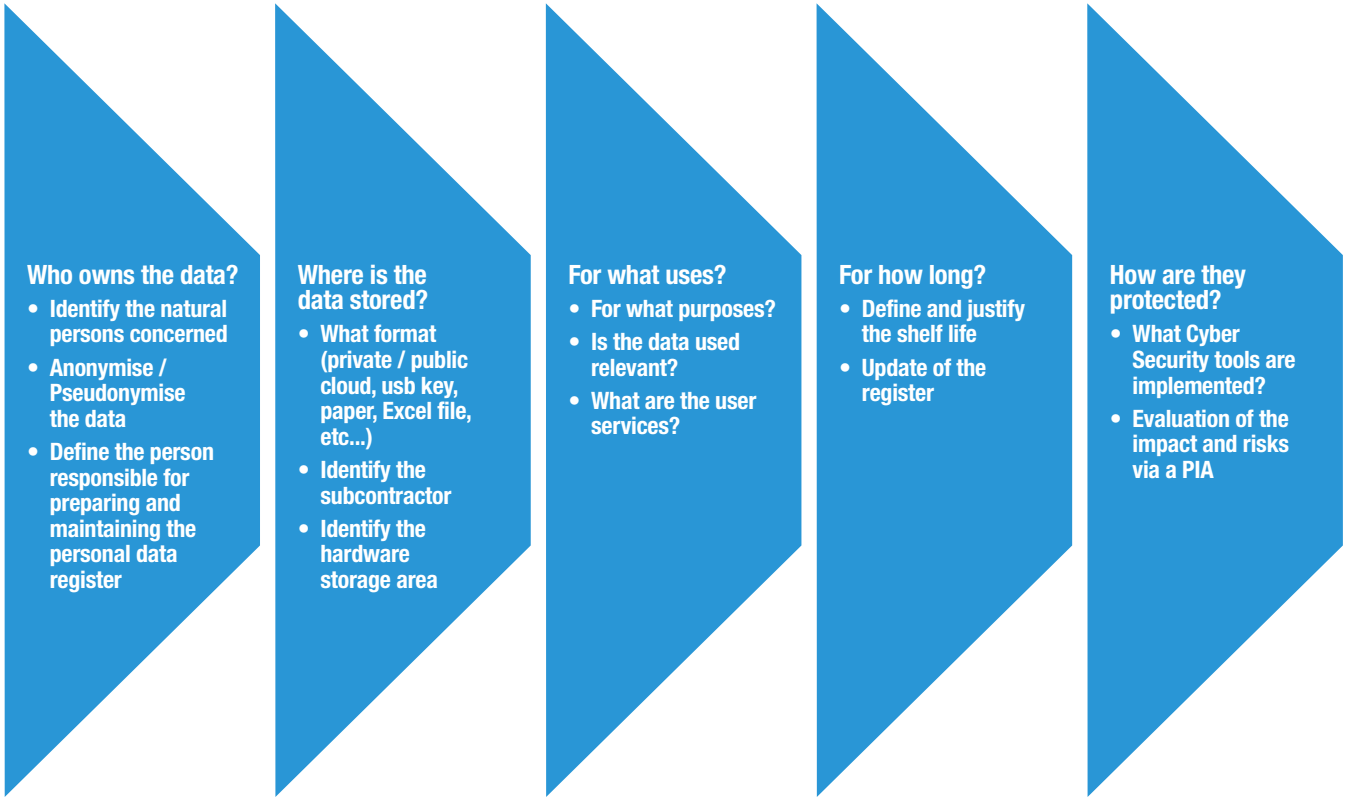
In this article, we will study how to apply this regulation to financial data in accordance with previous regulations.

GDPR: A mandatory framework with an international scope

Like FACTA's regulation for US citizens' taxation or the "*RIA Compliance Rules*" that define certain obligations while using the US Dollar in financial transactions, GDPR is based on articles 7 (*Respect for private and family life*) and 8 (*Protection of personal data*) of the Charter of The Fundamental Rights of the European Union. It thus protects all European Union nationals within the Union and internationally.

GDPR came into existence on 25 May 2018 and companies have been given two years to identify their personal data uses and implement measures to ensure their protection.

In 1971, the Secretary of the United States Treasury, John Connally, said, "*The dollar is our currency, but it's your problem.*" On the same lines, in 2018, as



GDPR was implemented, we can declare, "*The European citizen's personal data is their data, but it's your problem.*"

Apart from the existing legal risks, the credibility, the e-reputation and consequently, the confidence that customers grant to financial institutions are the major stakes of the GDPR compliance.

A special challenge for the banking and the insurance sector

As banking and insurance-related activities become increasingly digitalised, the collection of the personal data of customers has also become routine, before and throughout the duration of the business relationship: both for commercial purposes and in compliance with Know Your Customer (KYC) obligations in the context of anti-money-laundering and financial crime, such as MIFID II/AML/LCB-FT.

What are the requirements of the General Data Protection Regulation?

Regarding the banking sector, the processing of personal data is part of the GDPR when the purpose or effect is[1]:

- Assessment of personal aspects or rating of a person (e.g. financial scoring);
- Automated decision-making;
- Systematic monitoring of people (e.g. remote monitoring);
- Sensitive data processing (e.g. health, biometrics, etc.);
- Data processing of vulnerable persons (e.g. minors);
- Large-scale processing of personal data;
- Cross-reference of all data;
- Innovative uses or the application of new technologies (e.g.: connected objects, Artificial Intelligence, Robotic Process Automation…); and
- Exclusion from exercising a right, engaging a service or a contract (e.g. blacklist).

If your data processing meets at least two of these nine criteria, you should first conduct a Data Protection Impact Analysis (DPIA), before starting the processing operations.

Concretely, while implementing GDPR, organisations must ask themselves the right questions in order to respect the rights of consumers – see diagram above.

The GDPR reserves to consumers one of the rights that may be in contradiction with the obligations relating to the various initiatives, such as anti-fraud/anti-money-laundering, etc., as for example:

- The management of consent: obtaining it in an informed manner and having the ability to provide tangible proof of its collection[2],
- The right to oblivion that requires the deletion of

> **HOW CAN BANKING AND INSURANCE COMPANIES COMPLY WITH GDPR REGULATIONS WITHOUT OVERRIDING THEIR PREVIOUS OBLIGATIONS?**

MEETING THESE REQUIREMENTS CALLS FOR THE DEVELOPMENT OF ORGANISATIONAL PROCESSES, INTEGRATING TOOLS AND SOLUTIONS

personal data; however, especially when it comes to implementing the KYC requirement, banking and insurance stakeholders are required to keep these data and make them available to the different institutions.

- The right of access to the data in the context of portability, which raises the question of which data can be transmitted between the data provided by the consumer and the data that may have been provided by other services, in particular with regard to corporate solvency and bankruptcy.

Meeting these requirements calls for the development of organisational processes, integrating tools and solutions that allow for:

- Transparency for the customer: state clearly and explicitly beforehand the KYC investigation process (collected data, recipients, …) but also inform the customer about the points which can be subject to investigations and alerts;
- Collecting evidence of informed consent and its management i.e. archiving and preservation;
- Data accessibility: develop the transmission process for collected data to respond to requests for access to information as part of the KYC process. Moderation may be established as part of the bank's duty to safeguard information in the event of proceedings being opened, and at the request of a legal institution;
- The ability to operate data transferability; and
- The data retention period:
- Which process to apply for erasing personal data?
- What data to keep and in what format?
- Who will be responsible and which services will have access to this data and for what purpose?

and don't forget to remind the regulatory framework and the requirements for data retention.

The CNIL has responded to these obligations by issuing the Single authorisation AU-003[3] which translates as follows:

The personal nature of the processed data relates to:

"Client identification, where applicable, the owner beneficial in business relationship; the professional situation; the functioning of the account; the financial transactions or the subscribed products, the assets".

The recipients of this data as part of the management of access rights are:

- The national legal authorities (CNIL in France),
- The services responsible for the fight against money laundering within the body holding the data, namely the persons responsible for compliance,
- TRACFIN correspondents of the same banking group,
- The authorities of the State of the head office of the organisation, if it is a member of the European community.

CNIL mentions, "only persons who have the status of TRACFIN correspondent or registrant may receive communication of the existence of a declaration of suspicion and any information on the action that has been reserved by TRACFIN".

The duration of data retention is five years from:

- The closure of the account or the termination of the business relationship with respect to the data and documents relating to the identity of the customers,
- The execution of the transaction, concerning the data and documents recording the characteristics of the transactions mentioned in II of the article L561-10-2.

As a result, the players who are subject to the various anti-fraud regulations are required to provide answers about the organisational processes of collection and data processing, but also about the management of consent and the rights not needing consent, regarding the retention periods of data. For example, the right of access is exercised via an indirect right of access procedure, while guaranteeing the confidentiality of the data.

Implementation:

- Ensure compliance of regulatory requirements by auditing Customer Knowledge Processes (KYC) and analysing organisational and operational models;
- Analyze the impact of customer data through the development of Privacy Impact Asset (PIA) and the maintenance of appropriate registers;
- Develop procedures to notify public institutions within 72 hours and then inform the persons concerned; and
- Analyze risks (economic, organisational, financial), internal and external fraud, and the image and information systems in the context of data processing.

A collective collaboration of organisations for the processing of intra-group data in several states of Group 29 (G29) in the European Data Privacy Board (EDPB)

Banking and insurance companies are free to carry out internal arbitration concerning the processes to be implemented in the context of data sharing between the different departments. In order to facilitate these processes, the Community of the Article 29 (G29) Group, brings together private players and European public institutions in charge of monitoring these data, proposed rules and best practices in order to facilitate the exchange of information between officials within the same multinational.

The legal foundation is based on Articles L511-34 and R 561-29 of the Monetary and Financial Code and the use of the Binding

Corporate Rules (BCR) tool.

This framework facilitates the relationship of the banking and insurance companies and "creates a safe harbor for transfers within a group acting as a subcontractor". This organisation has been replaced by the European Data Protection Board (EDPB) with the following missions:

- Harmonise and ensure that the rules of the European Union (EU) are applied uniformly within the Member States;
- Ensuring the consistent application of the Data Protection Directive;
- Adopt "policy documents to clarify the provisions of European legislative acts" and "provide stakeholders with a coherent interpretation of their rights and obligations";
- Make formal announcements according to the article 70;
- Issue binding decisions in case of disputes between authorities according to Article 64; and
- Develop a common doctrine of EU data protection authorities.

G29's recommendations have thus led to the simplification of the procedures for transmitting data between entities of the same group while complying with the obligations of security and confidentiality of the data. These adjustments should allow to reconcile the duty of vigilance in the fight against money laundering and the financing of terrorism.

Conclusion

In conclusion, GDPR is not an impediment to the previous regulations and provides an additional guarantee against data leakage.

One of the keys to success is the transparency that the private sector players in the banking and insurance sector must demonstrate by adopting a pedagogical approach.

The GDPR's implementation is the opportunity to explain in a transparent way the purpose of the various regulatory frameworks in order to deploy them within organisations.

By extension, this situation also concerns non-financial organisations subject to the same supervisory obligations in the fight against money laundering and anti-terrorism (lawyers, notaries, real estate subsidiaries of a banking establishment, etc.).

The bank, a financial safety vault, has now become a safety vault for sensitive personal data. ■

Footnotes:

1 CNIL, RGPD: points de vigilance, www.cnil.fr/fr/rgpd-points-de-vigilance

2 RGPD Moment de vérité, Emmanuelle Inacio, INSOL Europe Partners, Spring 2018

3 CNIL, Autorisation unique AU-003 Lutte contre le blanchiment par les organismes financiers www.cnil.fr/fr/declaration/au-003-lutte-contre-le-blanchiment-par-les-organismes-financiers

> **THE BANK, A FINANCIAL SAFETY VAULT, HAS NOW BECOME A SAFETY VAULT FOR SENSITIVE PERSONAL DATA**