Collective of Authors

EFPA

Digitalization Handbook:

The Financial Advisor in the New Digital Era

EFPA Handbook

Contents

Introduction

Parts

Contributors

Part II: Regulation, Compliance and Risk Management

Part II

Regulation, Compliance and Risk Management

Chapter 9

Data Protection in the Digital Financial Landscape: A Regulator's Perspective

Introduction

While it is undeniable that the digital transformation has brought numerous opportunities not only for organisations of the financial sector but also for their clients, it has also brought new challenges for the protection of personal data. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**General Data Protection Regulation**" or "**GDPR**") has been applicable for six years and the financial sector has also changed significantly in recent years with the increasing use of digital banking and electronic payments, the development of new technologies, which have led to financial innovation and the emergence of tools such as tokenisation of assets, financial instruments transferred via distributed ledger technologies, etc. …

As such, organisations of the financial sector currently face several challenges, of which the following article will analyse a select few. For example, the use of new technologies, commonly referred to as "**Fintechs**", entails the processing of personal data, at times at an unprecedented scale or in manner not expected by the data subjects and could therefore risk leading to a complication of existing issues, such as personal data being processed without

individuals' knowledge or a lack of control for data subjects. In addition, the financial sector faces a constantly evolving and ever more complex legal and regulatory framework that requires or encourages additional personal data processing activities. An overarching matter is, of course, the use of Artificial intelligence ("AI") systems, whether generative or not, which already now raises a number of questions in terms of compliance with the data protection framework.

1. Points of attention in the GDPR for digital finance actors

Financial personal data are not per se considered as "sensitive data",[1] but it is commonly accepted that such data merit a high level of protection, because the misuse thereof may entail serious impacts in the data subject's daily life (e.g. such data might be used for payment fraud).[2] In the context of payments, for instance, many types of personal data may be processed:

- actual payment data: identifiers of the means of payment used, amount of the transaction, date and time of payment, identity of the merchant, identity of the beneficiary, IBAN, the customer's fraud prevention score, etc.

[1] Financial data are not listed as a special category of personal data in Article 9 of the GDPR.

[2] Guidelines of the Article 29 Data Protection Working Party on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p.10.

- purchase or checkout data: characteristics of the products purchased, date and place of purchase, loyalty card details if applicable, etc.
- contextual or behavioural data (particularly in a digital context): geolocation data, characteristics of the terminal used, characteristics of the products explored prior to the purchase, the time spent browsing, etc.[3]

Financial transactions can also reveal "special categories of personal data" about an individual data subject[4] (e.g. racial or ethnic origin, political opinions, religious beliefs, trade-union membership, health or sex life), which are subject to specific, additional safeguards.[5]

It is worth recalling here certain basic principles relating to the processing of personal data which appear to be critical in the context of digitalised financial services.

First, personal data shall be processed lawfully, fairly and in a transparent manner for the data subject.[6] Transparency is an overarching obligation under the GDPR and applies throughout the whole life cycle of processing and aims to engender trust in the processes affecting individuals by enabling them to understand and, if necessary, challenge

[3] https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-white-paper_when-trust-pays-off.pdf

[4] As set out in Article 9 of the GDPR.

[5] EDPS Opinion 39/2023 on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Market, §24.

[6] Article 5.1, a) of the GDPR.

those processes.[7] On the one hand, trends towards outsourcing and digitalisation and, on the other hand, the increasing number of processing operations and actors in a complex ecosystem have made it difficult for individuals to have a clear view of the processing of their personal data.[8] It is therefore crucial that controllers in the digital finance market carefully set out the roles of the organisations involved in processing activities and consider which special elements must be included in order to fully comply with the transparency requirements of the GDPR (through the provision of information to data subjects, the communication with data subjects in relation to their rights under the GDPR and the facilitation of the exercise by data subjects of their rights).[9] Better transparency measures may lead to more trust in the organisation and reputation gains for Fintech companies and could even become a means of stimulating competition in the FinTech industry.[10]

According to the principle of purpose limitation,[11] an organisation must be clear from the outset why it collects personal data and what it intends to do with it. Clearly defining purposes allows organisations to determine the

[7] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 11 April 2018.

[8] Cf. EDPB Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, §§ 72 to 79

[9] Cf. Guidelines on transparency under Regulation 2016/679, endorsed by the EDPB, §8 and following.

[10] Gregor Dorfleitner, Lars Hornuf, Julia Kreppmeier, "*Promise not fulfilled: FinTech, data privacy, and the GDPR*", Electronic Markets, Volume 33, Issue 1, December 2023, available here: file:///C:/Users/JYN923/Downloads/s12525-023-00622-x.pdf

[11] Article 5.1, b) of the GDPR.

necessity of the personal data collected for each processing operation, thereby helping to reduce the personal data collected, in accordance with the principle of data minimisation.[12] An organisation can indeed only process the personal data that are necessary and proportionate in light of the purpose envisaged. Personal data should be also retained for no longer than is necessary for the purposes for which the personal data are processed (storage limitation).[13]

Accuracy of personal data is also one of the key obligations in the GDPR.[14] Organisations acting in the financial sector are also subject to strict regulatory obligations (e.g. AML/CFT), which may have a significant impact on the individuals. It is therefore essential to have data quality control mechanisms in place providing the highest possible level of accuracy of the personal data processed.

Data protection by design and by default also plays a crucial part in the digital context.[15] Data protection by design consists of incorporating appropriate technical and organisational measures, such as pseudonymisation, to implement data protection principles within an organisation in an effective manner and integrate safeguards into the processing. Data protection by default requires organisations to implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are

[12] Article 5.1, c) of the GDPR.
[13] Article 5.1, e) of the GDPR.
[14] Article 5.1, d) of the GDPR.
[15] Article 25 of the GDPR.

processed. This principle refers to establishing configuration values or processing options that are set or prescribed in a processing system, such as a software application, service or device, or a manual processing procedure that affect the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.[16]

As regards the rights granted by the GDPR to data subjects, an organisation must make sure that data subjects can exercise the following rights: the right of access, the right to rectification, the right to be forgotten, the right to withdraw their consent, the right to contest a decision based solely on automated processing, the right to object, the right to data portability and the right to restriction of processing.

It should be noted that the right of access is a top priority for the European Data Protection Board[17] ("**EDPB**") for 2024.[18] It is worth bearing in mind that the Court of Justice of the European Union ("**CJEU**") has adopted a broad interpretation of the right of access. The Court recently held that this right also includes the specific indications of each

[16] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, §41.

[17] The European Data Protection Board (EDPB) is composed of the heads of the national data protection authorities of the countries in the European Economic Area. It ensures that the GDPR is applied consistently and ensures cooperation, including on enforcement.

[18] https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_en

recipient of data (and not only the categories of recipients)[19] and log data about the consultation operations carried out on a data subject's personal data and concerning the dates and purposes of those operations.[20]

2. New regulations applicable to the financial sector: a trend towards data sharing

Regulatory pressure constantly grows for financial institutions with the increase of EU regulations and directives applicable to the financial industry, which directly or indirectly affect the processing of personal data (AML/CFT package, Financial data access and payments package, Data Act, Data Governance Act, AI Act, DORA, NIS2, …). In this context, it is important to bear in mind that the GDPR is not the only piece of legislation setting out data protection obligations for organisations.[21] In addition, many recent or upcoming legal acts contain specific provisions regarding data protection or require organisations to process personal data and thus to implement appropriate safeguards.

---

[19] Judgment of the Court of Justice of the European Union of 12 January 2023, *RW* v *Österreichische Post AG*, C-154/21, ECLI:EU:C:2023:3.

[20] Judgment of the Court of Justice of the European Union of 22 June 2023, *J.M.* v *Apulaistietosuojavaltuutettu*, *Pankki S*, C-579/21, ECLI:EU:C:2023:501.

[21] For example, any organisation recording telephone conversations must also comply with the Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

One of the most emblematic illustrations of the interplay between financial legislation and data protection is the AML/CFT legal framework. Although the GDPR and the AML/CFT rules may have mutual interests, such as the processing of adequate, relevant and accurate data, the implementation of the AML/CFT obligations can sometimes lead to frictions. The interplay between these two sets of rules may be delicate to operate and the controller, pursuant to the principle of accountability as defined in the GDPR, must be able to demonstrate that they only process personal data, which are adequate and relevant for the AML/CFT purposes. It is interesting to note that the recently adopted Anti-Money Laundering Regulation ("**AMLR**")[22] contains numerous references to data protection, including provisions about the processing of special categories of data and personal data relating to criminal convictions and offences, decisions resulting from automated processes, including profiling, or from processes involving AI systems, retention periods and deletion of personal data, data protection awareness. One of the innovations of the AMLR is the exchange of information in the framework of partnerships for information sharing.[23] This provision allows obliged entities, in the context of partnerships, to share information under certain conditions for the purpose of complying with their AML/CFT obligations. The concept of sharing of information has been

[22] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[23] Article 75 of the AMLR.

strongly criticised by the EDPB during the legislative process,[24] because it may result in a high risk to the rights and freedoms of natural persons. Even if information sharing is subject to more restrictive conditions in the recently adopted AMLR, many practical questions as to data protection remain open. However, it should be noted that data protection authorities may be consulted by the supervisory authorities under the AMLR in the regulatory verification process.

The Proposal for a Regulation on a framework for Financial Data Access[25] ("**FIDA**") fits into the broader European strategy for data[26] and is connected to the Digital Finance Strategy for the EU,[27] notably to create a European financial data space to promote data-driven innovation, including enhanced access to data and data sharing within the financial sector. The FIDA Proposal aims, among other things, to establish clear rights and obligations to manage customer data sharing in the financial sector beyond payment accounts. Whilst this proposal is still subject to discussions by the European co-legislators, it may be noted that the innovative nature of the data sharing activity, the sensitivity of the data involved and the implications it could

[24] EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations, 28 March 2023.

[25] Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554, COM/2023/360 final, 28 June 2023.

[26] https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[27] https://finance.ec.europa.eu/publications/digital-finance-package_en

have on the financial sector and on financial inclusion are at the centre of discussions. The European Data Protection Supervisor issued an Opinion on FIDA with a number of recommendations and urged financial supervisory authorities to cooperate with data protection authorities both on EU and national level.[28]

Data sharing is also a key element in other proposals. Presented in conjunction with FIDA, the Proposals for a Directive on payment services and electric money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009-110-EC ("**PSD3**") and a Regulation on payment services in the internal market and amending Regulation (EU) No 1093/2010[29] ("**PSR**") aim to amend and modernise the current Payment Services Directive (PSD2). Some of the issues raised by the EDPS[30] and the EDPB[31] relate to transaction monitoring mechanisms and fraud data sharing. While information sharing arrangements are a key measure to prevent and combat fraud, it should be stressed that such processing may also have an important impact on individuals' rights to privacy and data protection. Against

[28] EDPS Opinion 38/2023 on the Proposal for a Regulation on a framework for Financial Data Access, 22 August 2023.

[29] Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010, COM/2023/367 final, 28 June 2023.

[30] EDPS Opinion 39/2023 on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Market, 22 August 2023.

[31] EDPB Statement 2/2024 on the financial data access and payments package, adopted on 23 May 2024.

that background, the EDPB issued specific recommendations to the Council on specific conditions and limits for such data sharing and the inclusion of additional safeguards.

3. Artificial intelligence and data protection

Considering the "data-intensive nature" of many AI systems that generate content (e.g. by issuing individualised proposals for investment or insurance products), make predictions (e.g. by helping assess whether a person may receive a loan) or take a decision in an automated way (e.g. to detect abnormal behaviour to fight fraud), obligations of the GDPR, such as transparency, human control, accountability and liability over results, can be severely challenged.[32]

While the move to AI technologies has already been initiated by many actors in the financial industry and the EU AI Act[33] is not yet applicable, two recent decisions of the CJEU grant useful insights into the application of the GDPR to AI technologies.

---

[32] Cf. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021

[33] Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

On 5 December 2023, the CJEU analysed the development and use of a mobile IT application in the context of the Covid-19 pandemic by a company to whom the Lithuanian Ministry of Health had outsourced the activity.[34] The decision is important for AI, as it assessed whether "processing" of personal data also covers the use of copies of personal data for IT systems testing. The decision also deals with legal responsibility for the use of personal data by a mobile application.

First, the Court confirmed that the use of personal data for the purposes of the IT testing of a mobile application constitutes "processing" covered by the GDPR, unless such data have been rendered anonymous in such a manner that the data subject is not or is no longer identifiable, or unless it involves fictitious data which do not relate to an existing natural person. Although this case is not about AI, it is likely that the same conclusions could be drawn with regards to data used for training AI tools.

Furthermore, the CJEU ruled that the organisation, which had outsourced the development of a mobile IT application to another organisation, and which has, in that context, participated in the determination of the purposes and means of the processing of personal data carried out through that application, may be regarded as a controller, even if that organisation:

---

[34] Judgment of the Court of Justice of the European Union (Grand Chamber) of 5 December 2023, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos* v Valstybinė duomenų apsaugos inspekcija, C-683/21, ECLI:EU:C:2023:949.

1. has not itself performed any processing operations in respect of such data,
2. has not expressly agreed to the performance of specific operations for such processing or to the fact that the mobile application should be made available to the public, and
3. has not acquired the mobile application, unless, prior to that application being made available to the public, that organisation expressly objected to such making available and to the resulting processing of personal data.

On 7 December 2023, the CJEU handed down an important decision on the interpretation of the notion of "automated decision-making" (case C-634/21).[35]

As a reminder, Article 22 of the GDPR confers on the data subject the right not to be the subject of a decision solely based on automated processing, including profiling. In other words, the GDPR prohibits the use of automated individual decision-making and allows for it to be used only in limited situations, i.e. if it is necessary for the performance of a contract, provided for in the law or based on data subject's consent. The GDPR also sets out safeguards, such as the right of the data subject to contest the decision and to obtain human intervention in the decision. The aim of this provision is to protect individuals against the particular risks that automated decision-making present to their rights and

[35] Judgment of the Court of Justice of the European Union of 7 December 2023, *OQ* v *Land Hessen* (*SCHUFA Holding AG*), C-634/21, ECLI:EU:C:2023:957.

freedoms, such as risks of financial exclusion via price discrimination or a refusal to supply financial products.

The Court analysed the scoring activities of SCHUFA Holding, a private company providing credit information for clients, including banks. Scoring consists of a mathematical statistical method used to predict the probability of future behaviour, such as the repayment of a loan. SCHUFA Holding rejected the assertion that Article 22.1 of the GDPR would be applicable to the activity of companies such as SCHUFA, by arguing that its role was to produce an automated score, but that the relevant decision (e.g., whether the loan would be provided) was taken by the third-party bank.

Ultimately, the Court adopted a broad interpretation of the concept of "decision" and ruled that the automated establishment, by a credit information agency, of a credit score constitutes "automated individual decision-making" within the meaning of Article 22.1 of GDPR, in so far as the credit information agency's clients, such as banks, attribute a determining role to it when deciding whether to grant a loan.

This judgment has broad implications for the Fintech market. Companies providing digital services based on risk scores or probability values and using algorithms or other automated processes (e.g., risk scoring in the context of anti-money laundering services) could fall within the scope of Article 22 of GDPR depending on how the score is used for the final decision. The findings of the CJEU could also be applied in the context of AI-based decisions.

While waiting for more clarifications from the legislator and courts, certain data protection authorities, such as those

of Luxembourg,[36] Norway and France have launched regulatory sandboxes for AI projects to anticipate possible risks and issues linked to AI data management and to put in place appropriate preventive measures guaranteeing compliance with data protection principles.

Conclusion

The digital economy is built on trust between individuals and professionals, which also extends to the field of privacy and data protection. Keeping in sight fundamental principles of the GDPR such as transparency, purpose limitation, data minimisation or accountability from the very beginning of a processing of personal data is a first step to ensure effective data protection. These principles should guide companies when navigating the diverse regulatory requirements in the digital financial landscape in order to allow them to strike a well analysed balance between data protection requirements and considerations such as the fight against fraud and AML/CFT or fostering innovation. Considering this, collaboration between data protection authorities and financial sector regulators, along with the participation of industry stakeholders, would allow data protection authorities to maintain a proactive approach to data protection in the digital financial landscape.

[36] https://cnpd.public.lu/fr/professionnels/outils-conformite/sandbox.html

Barbara Giroud

Juriste

CNPD – Commission Nationale
pour la Protection des Données

Contributors

Authors

Barbara Giroud

Juriste
CNPD – Commission Nationale pour la Protection des Données

Barbara Giroud has been working for the Luxembourg Data Protection Authority (Commission Nationale pour la Protection des Données – CNPD) as a legal expert since 2019. She focuses on the application of the General Data Protection Regulation (GDPR) in the financial sector. She also participates in the European Data Protection Board (EDPB) financial matters subgroup activities. Prior to joining the CNPD, Barbara has worked as a lawyer in the litigation and IP/Technology law practices of international law firms in Luxembourg. She holds a Master's degree in European Business Law.

Partners

CNPD – Commission Nationale pour la Protection des Données

The CNPD is an independent public institution responsible for monitoring the application of the GDPR (and other legal texts containing specific provisions on the protection of personal data) in Luxembourg. The CNPD also advises the national parliament, the government and other institutions and bodies on legislative and administrative measures relating to data protection.