GDPR Compliance in Fintech: Defining Roles and Contractual Liabilities

Tatiana Kyttaroudi, Associate | 13 March 2025

Introduction

The fintech sector is inherently data-driven, relying on vast volumes of personal data for services such as Know Your Customer (KYC), fraud detection and Anti-Money Laundering (AML) compliance. While data is at the heart of innovation in fintech, the General Data Protection Regulation (GDPR) imposes stringent requirements, seeking to balance data protection with the efficiency of financial services. Ensuring compliance within fintech is particularly challenging due to service fragmentation and outsourcing. Understanding the various GDPR roles, I.e. Controllers, Processors, Joint or Independent Controllers, is essential for ensuring legal certainty and mitigating compliance risks.

Roles in Data Processing

Data Controllers & Processors

Under the GDPR, a Data Controller determines the purposes and means of processing personal data. In the fintech sector, banks, payment service providers, and crypto-asset service providers (CASPs) typically assume this role, ensuring compliance with GDPR principles (Article 5) and informing data subjects about processing activities and their respective rights. A Data Processor by contrast acts on behalf of the Controller and executes processing activities under contract. Fintech companies frequently outsource functions to third party providers, such as identity verification platforms (IDV) cloud services providers (IaaS, PaaS, SaaS, FaaS) and call centers, which typically qualify as Processors. The GDPR mandates Data Processing Agreements (DPAs) between Controllers and Processors, setting out security measures, breach notifications and sub-processing limitations. If a Processor exceeds its mandate and independently determines the purposes and means of processing activities, it may be reclassified as a Data Controller, thereby incurring direct liability.

This principle has been affirmed in decisions, such as Decision 49/2011 of the Hellenic Data Protection Authority, which held that entities initially designated as Processors, such as debt collection agencies, may be deemed Controllers if they process data for their own independent purposes. The greater of the decision-making autonomy of a Processor, the higher the likelihood that it will be considered a Joint or Independent controller, as described below.

Legal Reasoning of the Court

Joint vs. Independent Controllers

A Joint Controller relationship arises when two or more entities jointly determine the purposes and means of processing. This is common in open banking under the Revised Payment Services Directive (PSD2), where banks and fintech firms collaborate on Payment Initiation Services (PIS) or Account Information Services (AIS). In such scenarios, both parties share liability under Article 26 of the GDPR. Other examples include BNPL (Buy Now, Pay Later) partnerships and crypto exchanges cooperating with banks on AML compliance. Conversely, Independent Controllers process data for their own distinct purposes. For instance, credit scoring agencies receive financial data from banks but operate autonomously in assessing creditworthiness. On the same note, data transfers to public authorities or financial databases (e.g., ΤΕΙΡΕΣΙΑΣ Α.Ε., Greece's credit bureau) do not establish a Joint Controller Relationship but rather separate Controller responsibilities.

Third Parties and Recipients

Under the GDPR, the terms third party and recipient (distinct notions) refer to entities not directly involved in processing under the Controller's authority. n fintech, recipients may include debt collection agencies, claims management firms operating under Law 4354/2015 or affiliated insurance providers.

The GDPR's transparency requirements mandate that data subjects be informed about the recipients of their personal data (Art. 13 and 14). Following the example of ΤΕΙΡΕΣΙΑΣ Α.Ε., the recipient of the data that it processes are banks and other financial institutions, credit card management companies, leasing and factoring companies, but also natural or legal persons, or associations of persons under the Civil Code, engaged in commercial, industrial, craft, agricultural, or other businesses operating within the Greek territory or in another EEA country (including Switzerland), according to the Τ.Σ.Ε.Κ. system.

Contractual Compliance Obligations

To achieve GDPR compliance, fintech companies must establish robust contractual frameworks that clearly define roles, obligations and liabilities in data processing:

- **Data Processing Agreements (DPAs)** (Article 28 of the GDPR) are required between Controllers and Processors, specifying security measures, sub-processing restrictions, and audit rights. The European Commission has introduced its Standard contractual clauses for controllers and processors in the EU/EEA (in short, its DPA template) in June 2021, for the facilitation of full compliance with the data protection framework.
- **Joint Controller Agreements (JCAs)** (Article 26 GDPR) define responsibilities for data protection, subject rights handling and liability, while
- **Data Sharing Agreements (DSAs)** govern transfers between Independent Controllers, ensuring legal basis and transparency.

Fintech-Specific Compliance & AI Challenges

KYC & AML Regulations

Fintech firms must comply with stringent KYC and AML obligations. In Greece, credit institutions subject to Art. 3 par. 2 of Law 4557/2018. conduct KYC checks by accessing data from databases of public bodies, such as ΑΑΔΕ or ΕΡΓΑΝΗ and the very KYC process is conducted in the eGov-KYC app, which is developed and operated by the General Secretariat for Information Systems of Public Administration under the Ministry of Digital Governance.In this case, Art. 10 of the Ministerial Decision 9747 ΕΞ 2021/2021, designates the Ministry of Digital Governance as the Data Controller. For outsourced KYC providers, third-party platforms act as Processors, handling customer onboarding and identity verification on behalf of financial institutions.

UPSD2 & PCI-DSS Security Obligations

Under PSD2, third-party providers, including PISPs and AISPs, must ensure explicit customer consent before accessing bank account data (Article 94 par. 2 of PSD2), but also for the transaction to be considered authorised (Art. 64 PSD2). Furthermore, GDPR principles of purpose limitation and data minimisation apply, restricting data use strictly to the requested service. To mitigate security risks such as phishing and fraud, PSD2 mandates Strong Customer Authentication (SCA) and secure data transmission standards. Additionally, compliance with the Payment Card Industry Data Security Standard (PCI-DSS) requires encryption, access control measures and regular vulnerability testing for fintech firms handling payment card data.

AI, Credit Scoring & Automated Decision-Making

AI-driven financial services, including **automated credit scoring**, **fraud detection and identity verification (IDV),** pose significant compliance risks under Article 22 of the GDPR. Also, the **EU AI Act** will impose stricter transparency and bias mitigation requirements, adding to the compliance burden for fintech firms.

Conclusion

Given the increasing complexities of AI, data protection and intersecting regulatory frameworks, fintech companies must take a proactive approach to compliance. Engaging specialised legal professionals and Data Protection Officers (DPOs) in the drafting of data processing agreements, privacy policies and compliance training programmes is essential. Ensuring robust legal frameworks not only mitigates regulatory risk but also enhances competitiveness by fostering trust and innovation in financial services.

Key contacts

Dr. Dimitris Tsibanoulis
Senior & Managing Partner
d.tsibanoulis@tsibanoulis.gr

Tatiana Kyttaroudi
Associate
t.kyttaroudi@tsibanoulis.gr

Tsibanoulis & Partners Law Firm

18 Omirou St.
106 72 Athens | Greece

T: +30 210 3675 100

W: tsibanoulis.gr