Fintech e-book 2024

Fintech security and regulatory compliance best practices 2024

Fintech compliance stats

Stats

64%

of fintech’s main website failed GDPR compliance assessment.

62%

of fintech's main website failed the Payment Card Industry Data Security Standard (PCI DSS) compliance test.

83%

Vulnerabilities and security issues of different severity were identified in 83% of tests conducted on software systems and applications.

56%

Tests have shown that 56% of the mobile app back ends have serious misconfigurations or privacy issues related to SSL/TLS.

Fintech companies, like other technology-driven businesses, are subject to increasing regulatory oversight. They are subject to the same rules as traditional institutions that provide financial services. Fintech companies should be compliant with all anti-money laundering, data protection, and know-your-customer rules according to their activities.

In the European Union, payment services are regulated by the Payment Services Directive 2 (PSD2), and alternative finance firms engaged in the trade of transferable securities are subject to the Markets in Financial Instruments Directive (MIFID). There are also laws and regulations not specific to financial services but which fintechs are subject to, such as the EU General Data Protection Regulation.

Table of contents

GDPR compliance

GDPR

As the European Commission states, the underlying intention of GDPR Compliance is to "give citizens back control over their personal data, and to simplify the regulatory environment for business”.

Who does GDPR apply to?

General Data Protection Regulation applies to all organisations which provide goods and services for EU citizens and process their personal data.

Article 3 of GDPR regulations explains the territorial scope:

01

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

02

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

03

This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Main GDPR requirements to consider in advance

01 You must document data protection-related processes and policies and keep records to demonstrate compliance.

02 Article 32 of GDPR highlights that organisations must implement “technical and organisational measures to ensure a level of security appropriate to the risk”. To comply with these requirements, you have to conduct regular risk assessments, have policies, and physical and technical measures in place.

03 Assess the strength of controls and programmes. Make sure to test and assess the sufficiency of critical security measures and programs in place. Not only the technology but people and processes, too. Ensure to test for vulnerabilities and weak spots regularly and address any gaps. Not only will it make you compliant in the eyes of the law, but it's never a bad idea to continuously be evolving your security.

04 Provide users with notifications and access to an unambiguous privacy statement with detailed information on data processing every time data collection occurs.

05 Purpose limitation requirement: personal data can be processed for only specified and legitimate purposes with user notification. The legal basis for data processing in fintech companies is user consent and contractual necessity.

06 Take care of enhanced customers' rights. With new data portability rights, customers can switch service providers and demand the return of data-controlled, not only personal data but also data generated during services and activities. The right to be forgotten enables a customer to require their data to be erased. This creates a challenge for blockchain-based fintechs conflicting with its immutability attribute. In a blockchain, right-to-be-forgotten can be realised by deleting data from the profiles, but any data that was sent in transactions can not be removed. Requirements for secure storage skyrocketed from here.

07 Integrate privacy and information security into your company’s technology and processing systems by design. Top security measures are:

- to ensure the ongoing confidentiality, integrity, and resilience of processing systems;
- ability to restore availability and access to personal data in case of an incident;
- pseudonymisation and encryption of personal data.

GDPR Non-Compliance Sanctions

Even if your organisation does not have a location in the EU, GDPR has extraterritorial application as it applies to any entity or data controller – inside or outside the EU – that monitors the behaviour or offers goods or services to EU residents, and therefore processes any of their personal data. The penalties for non-compliance include fines of up to 20 million euros or 4% of the firm’s worldwide annual revenue. The less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

S-PRO comments on GDPR compliance experience

S-PRO comments

When we worked on a global market-oriented project that included a payment gateway, we discovered that the main technical issue lay in the Data Processing Agreement and its user interactions. Every document point was followed by a checkmark. If the user didn’t comply with certain regulatory provisions, then architecture should be configured to filter and display content in accordance with positions ticked by a user in the agreement.

For the seamless realisation of these tasks, we chose to use Command Query Responsibility Segregation and Event Sourcing patterns. To ensure the security of stored data and its processing, we applied sharding for database geo-partitioning, which enabled us to split a massive database by country of origin and create individual databases for each country. That's really helpful in achieving GDPR compliance.

GDPR Compliance Readiness Checklist

- Encourage everyone in your organisation to seriously focus on data governance responsibilities.
  - Record keeping (art. 30)
  - Employee training (art. 5)
  - Appoint Data Protection Officer (art. 37)
- Make your privacy notes completely informative and unable to be misinterpreted (art.12-14).
- Provide data subjects with abilities to exercise their right for data access, portability, and processing restriction. (art.15-21)
- Consider both organisational and technical security measures for personal data protection, such as confidentiality, pseudonymisation, encryption. (art.32)
- Be prepared to report data breaches to affected data subjects and regulators within 72 hours of incident awareness.
- Establish the required policies and procedures
  - General Data Protection Policy
  - Processing customer data policy
  - Data Breach Escalation and Checklist
  - Guidance on privacy notices (more in art.5)
- Establish a legal basis to own and process personal data.
- Ensure privacy by Default and Design (art.25)
- Learn rules and mechanisms of data export outside the European Economic Area and prepare adequate contracts for third parties, if applicable. (art.28; art. 44-49)

PCI DSS compliance

PCI DSS compliance

Payment Card Industry Data Security Standards (PCI DSS) are required for fintechs that store and process sensitive card data online. It helps fintechs protect sensitive cardholder data and maintain consumer confidence.

Who does PCI DSS apply to?

The PCI DSS applies to any merchant or service provider that handles, processes, stores, or transmits credit card data.

PCI DSS requirements

Implementing and managing network security controls

Applying secure configuration to each component of the system

Protection of account data

Using cryptography methods to protect cardholder data in public networks

Shielding all systems from malicious software

Increasing and sustaining the security of all systems and software

Limiting system components and cardholder data access based on business necessity

User identification and authentication to access the system components

Restricting physical access to cardholder data

Monitoring and keeping track of accessing system components and cardholder data

Regular evaluation and testing of systems and network security

Aligning with organisational policies to support information security

PCI DSS big advantage

Fintech companies can focus on PCI DSS certification and/or use it as a framework to comply with different regulatory and industry requirements like GDPR, HIPPA, and numerous others. It also helps to assure third parties and stakeholders

PCI DSS non-compliance penalties

The Payment Card Industry has established fines of up to $500,000 per incident for security breaches when merchants are not PCI compliant.

S-PRO comments on PCI DSS compliance experience

S-PRO comments

When building a payment gateway for a telecommunications provider, we passed the PCI DSS compliance procedure for Level 3 (1M transactions per year) in the first attempt. It’s not the hardest one. Just follow the rules of practices for the development of solution software architectures and keep in mind that card data should be stored in a private segment separated from your main infrastructure. Develop strong procedures for monitoring and encryption.

For startups in the early stages, it may be difficult and costly to comply with PCI DSS standards from the very beginning. A more expedient way would be integration with already compliant systems like Visa Checkout or Masterpass. This way, startups can receive revenue for their products while paying fees to compliant systems, and, in the meantime, work on their own infrastructure to meet PCI DSS standards directly.

Top payment gateway APIs

Stripe API

Accept, process, and manage online payments and subscriptions.

PayPal API

Accept PayPal and credit card payments on the web or on mobile.

KeyPay API

KeyPay is a payroll system that caters specifically to Australian businesses.

Noodlio Pay API

A simple solution for accepting payments on your website, in your app, or elsewhere on the web.

Adyen API

Credit card processor that hosts payment forms for sellers.

BIPS Invoice API

Accept cryptocurrency payments.

Square API

Accept, process, and filter online payments for your e-commerce.

Paybook API

An API that connects bank, utility, and government agency accounts.

PayMill API

Accept credit card payments from customers around the globe.

Other important regulations for Fintech startups: EMI & PSP

Important regulations

EMI licence

Electronic Money Institution is a licence to issue electronic money. It allows fintechs to issue their own quasi-currency, which can be used outside the payment system's website. The issued electronic currency can be withdrawn and converted into any other currency. The licence also permits the use of quasi-currency to service third-party payments, such as in e-commerce.

Electronic Money Institution is almost a bank, but without the right to issue loans. The license enables fintechs to open sub-accounts for customers within their bank account, effectively creating an 'electronic wallet.' However, the 'know your customer' (KYC) rule applies to these structures, albeit with modified operational limits.

PSP licence

A payment service provider (PSP) offers merchants online services to accept electronic payments through various methods, including credit cards, direct debit, bank transfers, and real-time transfers based on online banking. Typically, PSPs operate as a SaaS model, providing a single payment gateway that supports multiple payment methods for merchants. Typically, a PSP can connect to multiple acquiring banks, cards, and payment networks.

In many cases, the PSP will fully manage these technical connections, relationships with the external network, and bank accounts and therefore takes care of the technical processing of payment methods for online shops. This reduces merchants' dependence on financial institutions and frees them from the task of directly establishing these connections, especially for international operations. By negotiating bulk deals, PSPs can often offer lower fees.

Key elements to consider to become a payment service provider

01 Select white-labeled or exclusive payment gateway software

02 Implement own server infrastructure or use a PCI-compliant host

03 Take care of PCI compliance and card storage

04 Select processors and banks for transaction processing

PSD2 compliance

PSD2 compliance

PSD2 aims at making consumer access to their banking data simpler and driving fintech innovations by encouraging banks to exchange customer data securely with third parties.

Who does PSD2 apply to?

PSD2 applies to any payment that occurs or even travels through the European Economic Area.

Key points for Fintechs

01 Strong customer authentication

02 Regulatory technical standards

03 Open Banking APIs with access through two models of accreditation Account Information Service Provider (AISP) and Payment Initiation Service Provider (PISP).

Open-banking created value

01 Use third-party capabilities in addition to main offerings

02 Capitalise on consumer behaviour and store consumer preference data

03 Simplify the multi-factor authentication process

PSD2 Compliance Checklist

For account-holding institutions

- Create APIs to access transactional payment data with:
  - Multi-factor and continuous customer authentication
  - User behavioural analytics Real-time access and access control
  - Fraud monitoring
- Provide access to account (XS2A)
- Strong authentication
- Know your customer
- Implement and manage network and API security infrastructure

For third-party providers

- Get a PISP or AISP license
- Establish a trust framework with banks
- Offer secure applications based on user consent and fraud monitoring
- Implement a consumer identity and access management solution to facilitate:
  - User behavioural analytics
  - Provide Access to Account (XS2A)
  - Set up IAM or CIAM solution
  - Anti-money laundering

More Fintech APIs to consider

BIN – Issuer Identification Number database API

This API endpoint returns the information of BIN/IIN numbers.

Worldbank API

Access extensive ecosystem to accelerate your development process.

Yahoo Finance API

Helps to query for all information about finance summary, stocks, quotes, movers, etc.

Cloudserve Converter API

An API to convert between, extract, and parse numerous common generic and bank-specific financial message formats.

Zirra API

Makes non-traditional data usable for investors to reduce risk, increase return, and boost overall educated decisions.

Twelve Data API

Access to historical and real-time stocks, forex, and cryptocurrencies quotes.

MiFID II compliance

MIFID II compliance

Markets in Financial Instruments Directive (MiFID II) is part of broader measures used in response to the financial crisis. They cover the European Markets Infrastructure Regulation (EMIR) and the Securities Transactions Regulation (SFTR) seeking to make the OTC derivative market safer and regulate the shadow-banking sector in the EU.

Who does MiFID II apply to?

It covers all natural and legal persons who perform investment services and activities using financial instruments, as a regular occupation or business, and on a professional basis. MiFID II covered services, i.e.:

01 Investment advice to clients

02 Management of client portfolios

03 Execution of clients' orders on financial instruments

04 Reception and transmission of orders on financial instruments

05 Dealing with own account

06 Market making

07 Underwriting

08 Placing of financial instruments

09 Operating trading facilities

Single Euro Payments Area (SEPA compliance)

SEPA compliance

SEPA is a payment-integration initiative of the European Union for the simplification of money transfers denominated in euros. As a result of faster transfers and reduced bank charges, SEPA is estimated to generate EUR123 billion of savings over six years.

It allows European consumers, businesses, and public administrations to make and receive the following types of transactions under the same basic conditions:

Credit transfers **Direct debit payments** **Card payments**

Who does SEPA apply to?

SEPA covers any organisation in the European Union and other European countries where transactions in euros are provided.

The new SEPA Credit Transfer and DD schemes require the use of the International Bank Account Number and Bank Identifier Code as well as the XML ISO 20022 standardised file format to exchange bulk payment and DD files between banks and corporates.

SEPA Compliance Readiness Checklist

- SEPA credit transfer requires ISO 20022 XML format in the SEPA zone.
- SCT requires the Remitter to provide IBAN details of the Payees/Beneficiaries.
- Make sure your messaging formats (XML) and processes (ability to store IBAN & BIC, ability to handle 'R' transactions) are SEPA compliant.
- Get a Creditor Identifier from your bank.
- Gather and/or convert details of your payers in BIC and IBAN formats.
- Implement data validation algorithms.
- Migrate any existing mandates to the Core scheme.
- Create new mandates for existing Direct Debits for the B2B scheme.
- Notify existing customers of your migration to SEPA Direct Debit.
- Check that your back office or ERP system is able to manage SEPA data.
- Plan for a testing phase in your implementation.

SEPA Eligibility Checklist

Applicants must at all times:

- Be active in providing banking and/or payment services to customers;
- Be active in providing Payment Accounts used for the execution of payments, holding the Funds needed for the execution of payments, or making the Funds received following the execution of payments available to customers;
- Be either incorporated and licensed in a SEPA country or territory or licensed by an appropriate EEA regulatory body;
- Be able to pay the debts as they fall due, and not be insolvent as defined in accordance with any insolvency law applicable;
- Maintain a sufficient level of liquidity and capital under regulatory requirements to which it is subject;
- Be able to meet rating or other criteria set under SEPA terms from time to time to establish the ability to meet its financial obligations
- Fully comply with applicable regulations on money laundering, sanctions restrictions and terrorist financing;
- Participate, or be eligible to participate, directly or indirectly, in one or more Clearing and Settlement Mechanisms (CSMs);
- Develop and maintain operational and risk control measures appropriate to the business.

ISO 20022

● ISO 20022

ISO 20022 is the universal financial industry message scheme developed in 2004 under the ISO Financial Services Technical Committee 68 (TC68). There are currently over two hundred and twenty ISO 20022 standards adoption initiatives in the global financial services industry.

Value of ISO 20022 for Fintech

01 Open and collaborative standard – a key enabler for the future of open banking. Any organisation can make use of standards and design messages in a collaborative way as open standards are not controlled by a single commercial interest and are publicly available on the ISO 20022 website.

02 Rich and proven data model – allows any user to create ISO 20022 messages and data structures, including new contents in the business model to define the financial business concepts, processes, flows, and inter-relations. The ISO 20022 repository contains reusable concepts and data components that could be reused to create a business data record in a distributed ledger.

03 Tech-neutral business language – ISO 20022 provides the means to achieve uniform and unambiguous interpretation of the data exchanged among users, regardless of different technologies in use within and across the financial industry. Based on universal business models, the common standards can be enhanced to incorporate features of new technology and can be made tangible by adopting a physical standard. For this reason, ISO 20022 does not necessarily have to be expressed in XML messages and could, for example, also be rendered in JSON.

04 Global interoperability – ISO 20022 facilitates interoperability at three.

ISO/IEC 27001

ISO/IEC 27001

ISO/IEC 27001 is an internationally recognised standard for a holistic approach to information security covering three key areas: technology, processes, and people. ISO/IEC 27k series enables companies to manage the security of valuable information assets, including but not limited to customer data and the company’s data and assets.

Businesses certified under ISO 27001 achieve returns execution efforts, improving security as well as demonstrating compliance. In addition, it is a global benchmark, which demonstrates clients' and partners' unquestionable confidence in information security management and privacy standards.

ISO 27001 uses a top-down, risk-based approach. It defines a six-part preparation procedure

01 Define a security policy

02 Define the scope of the ISMS

03 Conduct a risk assessment

04 Manage identified risks

05 Select control objectives and controls to be implemented

06 Prepare a statement of applicability

Documentation, responsibility management, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organisation

Compliance as a result of good security

Information security

In order to comply with various industry & regional legal regulations, it is necessary to understand your security vulnerabilities and address them in a proper manner. The process of understanding and evaluating risk improves decision-making in business. Conduct regular compliance and information security assessments.

01 Web and mobile application penetration testing

02 Configuration reviews

03 Source code reviews

04 Evaluate protection for high-value systems, including external and/or internal cybersecurity measure

05 Reverse engineering

06 DDoS benchmark tests

07 Compliance for information security requirements e.g., ISO 27001:2013, PCI:DSS

08 Business continuity/recovery capabilities audit

After highlighting the relevant risks, future investments can be planned more effectively, along with any necessary changes in the environment of existing security programs or technology usage.

Electronic identification and trusted services (eIDAS) regulation

Electronic identification

eIDAS regulates electronic identification and trust services for digital transactions in the EU's Single Market. eIDAS standards provide electronic transactions with the same legal standing as those conducted on paper. eIDAS embody principles of information security, interoperability transparency, and drive innovations.

eIDAS provides a regulatory environment for the next aspects of electronic transactions

01 Requirements for advanced electronic signatures: it must be linked to the signatory in a unique way and be capable of providing the signatory identification; data used for signature creation is under signatory sole control; any subsequent change in the data should be detectable; there should be a certificate for electronic signature, and proof that confirms the identity of the signatory and links the electronic signature validation data to that person.

02 A qualified digital certificate attests to the authenticity of an electronic signature.

03 The activity of Trust Service Providers that creates, validates, and verifies electronic signatures, timestamps, seals, and certificates.

eIDAS advantage for Fintechs

01 eIDAS is helpful in ensuring compliance with Know-Your-Customer and Anti-Money Laundering policies. It strengthens security levels and fastens checks.

02 eIDAS embraces innovations by keeping technological neutrality. Fintechs can create their own solutions and use any kind or combination of technologies as long as it ensures achieving regulatory standards.

Key elements of eIDAS

eIDAS

Electronic Identification and Trusted Services (eIDAS) include two elements: Electronic Identification (eID), which provides a trustworthy identification method across the EU, and Trust Services for Electronic Transactions, which secure online activities.

Electronic identification (eID)

eID is a digital identification method used in electronic transactions through eID schemes. It allows identifying individuals and entities across EU countries.

Trust services for electronic transactions

Trust services cover a range of digital tools for ensuring the security and protection of online activities.

01 **Electronic documents** include all types of content stored digitally, whether it's sound, visual elements, or text.

02 **Electronic signatures** are equivalent to written ones and can be accepted with the physical presence of the signee.

03 **Electronic seals** confirm the authenticity of legal entities, their documents, and their transactions in digital relations.

04 **Time stamps** definitively indicate the time and date of electronic transactions, confirming their legal validity.

05 **Electronic delivery services** are used to secure and maintain the confidentiality and integrity of documents in the course of their transmission.

06 **Website authentication** is performed through certificates issued by qualified trust service providers.

AML policy

AML policy

Anti-money laundering (AML) regulations and procedures prevent criminals from disguising illegally obtained funds as legitimate income. AML requirements vary by country but are generally based on the recommendations of the Financial Action Task Force (FATF), the global watchdog for money laundering and terrorist financing.

The risk-based approach is required in sectors exposed to financial crimes, such as:

01 Money or value transfer service sector

02 Trust and company services sector

03 Banking sector

04 Payment services sector

05 Security sector

06 Life insurance sector

To meet AML requirements, Fintech must build programs based on AML pillars:

01 Internal controls checkup

02 Independent testing review

03 AML compliance officer checkup

04 Training checkup

05 Customer due diligence

AML penalties

AML penalties

In 2023, the most AML fines were imposed on the United States, United Kingdom, and Switzerland. Among specific organisations, the largest fine was imposed on Binance – $4.3 billion for engaging in money laundering, unlicensed money transmitting, and sanctions violations. Crown Resorts was fined $450 million for breaches of Australian AML laws. Deutsche Bank and its US affiliates received a fine of $186 million for failure to address money laundering issues.

01 AML-related infractions led to $8 billion in fines for global financial institutions in 2022.

02 Strong AML policy is one of the key factors banks consider before entering the partnership with a fintech company.

03 Firstly, fintechs must build a rigorous risk assessment system. Implementing KYC also helps mitigate risks during the onboarding stage.

Know your customer (KYC) compliance

Know your customer

The KYC program is essential for assessing the risks posed by clients by verifying their identity and monitoring their financial activities. Knowing your customer programme builds strong ground for AML compliance.

Who is the subject of KYC?

Banks, financial institutions, and any other institution that touches money.

The features KYC program requires

01 Customer identification program (CIP)

02 Customer due diligence

03 Enhanced due diligence

04 Constant monitoring of customer’s account-related and transactional activities, including a Suspicious Activity Report (SAR)

05 Established KYC procedures for corporate accounts with AML/KYC checks

06 Know your customer’s customer (KYCC) for B2B clients

07 Digital verification techniques

08 Underlying risk management strategy

Non-compliance with KYC and sanctions violation

12 of the world’s top 50 banks were fined for non-compliance with AML, KYC, and sanctions violations in 2019. By country, Switzerland was the biggest offender after a tier-one Swiss bank received the biggest single fine at $5.1 billion for AML breaches by the French Criminal Court.

Peer-to-peer (P2P) lending regulations

Peer-to-peer

Since its inception, the P2P lending market in the EU has been under-regulated and underdeveloped. At the end of 2022, the European Crowdfunding Service Providers Regulation (ECSPR, Regulation 2020/1503) was finally adopted. It includes uniform rules for all the EU States. They govern investment and lending crowdfunding services for businesses. Each financial platform under this Regulation can apply for a single authorisation with an EU passport to provide their services across the European Union. All EU P2P sites need to be licensed as “Crowdfunding Service Providers” to be able to operate.

Main objectives of EU P2P finance regulatory framework

1. Enable European Crowdfunding platforms to scale up by making it easier for crowdfunding platforms to operate across the EU.
2. Increase investors’ trust to engage in platforms operating across borders by increasing transparency and strengthening the integrity of platforms.

Key benefits of the European crowdfunding service providers regulation

01

Funds protection
Licensing requirements for CSPs ensure that the funds are stored by authorised providers, better protected, and segregated from other assets.

02

Detailed loan information
Commercial borrowers have to submit “key investment information sheets” with data about each loan, including its specific features and risks.

03

No conflicts of interest
Loans linked to P2P sites, their stakeholders, or related individuals are prohibited to avoid any conflicts of interest.

04

Discouraging criminal behaviour
Strict requirements for licensing, as well as the cost, effort, and transparency regulations that come with them, deter scammers from engaging in P2P lending.

05

Public business continuity plans

Companies have to provide arrangements that will work in the event of a company’s failure and ensure the continuing provision of critical services.

06

Full performance disclosure

Providers have to disclose 36 months of default histories and valuations of loans, which can help investors evaluate their projected returns better.

07

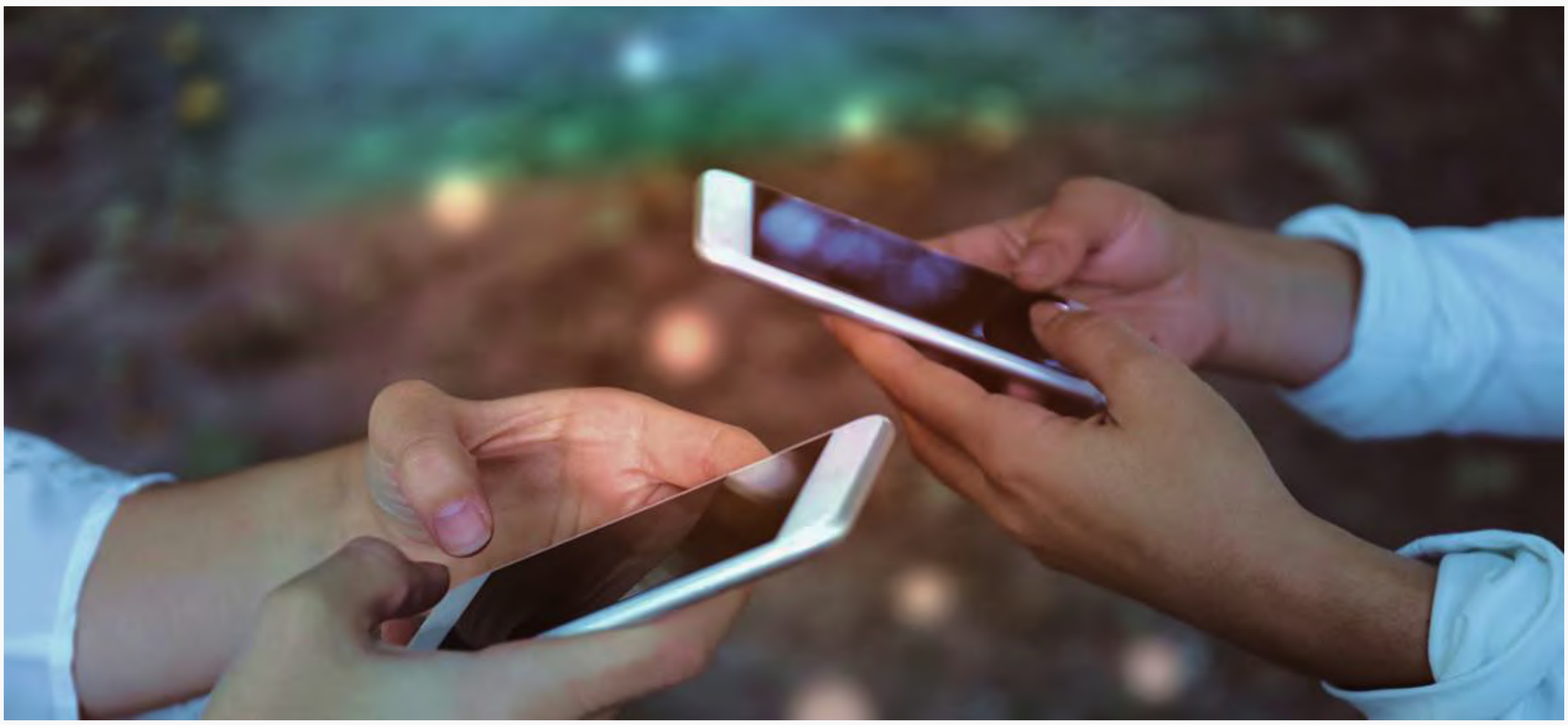
Consistent standards across the EU

The standards for P2P lending have varied greatly in different EU members before, but with the new Regulations, they are standardised and unified across the Union.

08

Public register of CSPs

The public register of approved CSPs is published and maintained by the European Securities and Markets Authority (ESMA).



Mentioned regulation articles

Sources

EU General Data Protection Regulation (GDPR)

Article 3 "Territorial scope"

https://www.privacy-regulation.eu/en/article-3-territorial-scope-GDPR.htm

Article 32 “Security of processing”

https://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm

Article 84 "Penalties"

https://www.privacy-regulation.eu/en/article-84-penalties-GDPR.htm

Article 30 "Records of processing activities"

https://www.privacy-regulation.eu/en/article-30-records-of-processing-activities-GDPR.htm

Article 37 "Designation of the data protection officer"

https://www.privacy-regulation.eu/en/article-37-designation-of-the-data-protection-officer-GDPR.htm

Article 5 "Principles relating to processing of personal data"

https://www.privacy-regulation.eu/en/article-5-principles-relating-to-processing-of-personal-data-GDPR.htm

Article 12 "Transparent information, communication and modalities for the exercise of the rights of the data subject"

https://www.privacy-regulation.eu/en/article-12-transparent-information-communication-and-modalities-for-the-exercise-of-the-rights-of-the-data-subject-GDPR.htm

CHAPTER III – Rights of the data subject

Article 13

https://www.privacy-regulation.eu/en/article-13-information-to-be-provided-where-personal-data-are-collected-from-the-data-subject-GDPR.htm

Article 14

https://www.privacy-regulation.eu/en/article-14-information-to-be-provided-where-personal-data-have-not-been-obtained-from-the-data-subject-GDPR.htm

Article 15

https://www.privacy-regulation.eu/en/article-15-right-of-access-by-the-data-subject-GDPR.htm

Mentioned regulation articles

Sources

Article 25 "Data protection by design and by default"

https://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm

Article 28 "Processor"

https://www.privacy-regulation.eu/en/article-28-processor-GDPR.htm

PCI DSS

PCI Security Standards Council

https://www.pcisecuritystandards.org/document_library

PSD2

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

MIFID II

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065

eIDAS

The Regulation (EU) N°910/2014 on electronic identification and trust services

https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

About S-PRO

Who we are

S-PRO is an innovative software development and consulting partner. We offer fintech companies solutions that enable them to pack innovative business models into flexible, adaptable, and secure technological products.

No legal advice is given herein. The provided compliance information is purely illustrative. Fintech companies should seek legal counsel for implementing compliance strategies due to their individual circumstances.

S-PRO provides advisory services solely on the technological side of financial software security.

Do you have any questions or need more details for your case?

Feel free to contact us

hi@s-pro.io