International Standard

ISO/IEC 27562

First edition
2024-12

Information technology — Security techniques — Privacy guidelines for fintech services

Technologies de l'information — Techniques de sécurité — Lignes directrices relatives à la protection de la vie privée pour les services fintech

Reference number
ISO/IEC 27562:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27*, Information security, cybersecurity and privacy protection.*

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Fintech refers to the use of ICT technologies across all financial service functions, for example, banking, payments and insurance.

Fintech represents the next wave of innovation for the financial service sector. Strong authentication technologies, emerging decentralized technologies like blockchain, analytical technologies for fraud detection and anti-money laundering compliance are changing digital financial services. Privacy aspects are the top priority in order to build trust and confidence in fintech services and applications and to protect financial infrastructure and customers.

AML (anti-money laundering) rules require the collection, processing and use of personal data as part of customer due diligence (CDD). Fraud detections require transaction monitoring, behavioural monitoring, internal data sharing (including within a group), external data sharing (including with regulators and other financial institutions), data sharing for outsourced arrangements; and cross-border processing of data (especially for international payments). Consumers want to be able to control access to, and usage of, their information.

This document draws upon the privacy principles and framework described in ISO/IEC 29100:2024 and the privacy impact assessment specified in ISO/IEC 29134:2023 to develop the guidelines for fintech services.

This document identifies regulations, such as anti-money laundering, fraud detection, and countering terrorist financing. It identifies all relevant stakeholder and privacy risks which are related to fintech services.

Information technology — Security techniques — Privacy guidelines for fintech services

1 Scope

This document provides guidelines on privacy for fintech services.

It identifies all relevant business models and roles in consumer-to-business relations and business-to-business relations, as well as privacy risks and privacy requirements, which are related to fintech services. It provides specific privacy controls for fintech services to address privacy risks.

This document is based on the principles from ISO/IEC 29100, ISO/IEC 27701, and ISO/IEC 29184, the privacy impact assessment framework described in ISO/IEC 29134, and the risk management guideline described in ISO 31000. It also provides guidelines focusing on a set of privacy requirements for each stakeholder.

This document can be applicable to all kinds of organizations such as regulators, institutions, service providers and product providers in the fintech service environment.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
actor
organization or individual that fulfils a role

[SOURCE: ISO 23234:2021, 3.4]

3.2
anonymization
process by which *personally identifiable information (PII)* (3.15) is irreversibly altered in such a way that a *PII principal* (3.17) can no longer be identified directly or indirectly, either by the *PII controller* (3.16) alone or in collaboration with any other party

[SOURCE: ISO/IEC 29100:2024, 3.2]

3.3
application programming interface
API
set of functions, protocols, parameters, and objects of different formats, used to create software that interfaces with the features or data of an external system or service

[SOURCE: ISO/IEC/IEEE 26531:2023, 3.1.1]

3.4
artificial intelligence
AI
discipline concerned with the building of computer systems that perform tasks requiring intelligence when performed by humans

[SOURCE: ISO/IEC 39794-16:2021, 3.6]

3.5
automated decision making
process of making a decision by automated means without any human involvement

3.6
control
measure that is modifying risk

Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.

Note 2 to entry: It is possible that controls do not always exert the intended or assumed modifying effect.

[SOURCE: ISO/IEC 27000:2018, 3.14]

3.7
de-identified dataset
dataset resulting from the application of a de-identification process

[SOURCE: ISO/IEC 20889:2018, 3.8]

3.8
fintech
digital innovations and technology-enabled business model innovations in the financial sector

3.9
fraud detection system
software as an application that supports monitoring, detection, and management of fraud or other misuse across users (e.g. customers), accounts, channels, products and other entities (e.g. kiosks)

Note 1 to entry: To deploy the fraud detection system, enterprise applications can integrate with a fraud detection engine that assesses the fraud risk of a transaction, from user navigation and application access, to any type of activity, such as a change of address, payment or retrieval of sensitive information.

[SOURCE: ITU-T X.1157:2015, 3.2.1]

3.10
governance
human-based system comprising directing, overseeing and accountability

[SOURCE: ISO/IEC 38500:2024, 3.3]

3.11
joint PII controller
personally identifiable information (PII) controller (3.16) that determines the purposes and means of the processing of *PII* (3.15) jointly with one or more other PII controllers

[SOURCE: ISO/IEC 27701:2019, 3.1]

3.12
know your customer
KYC
process to verify the identity of a customer in order to prevent financial crime, money laundering and terrorism financing

[SOURCE: ISO 12812-1:2017, 3.18]

3.13
machine learning
ML
process using computational techniques to enable systems to learn from data or experience

[SOURCE: ISO/IEC TR 29119-11:2020, 3.1.43]

3.14
malware
malicious software
software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system

EXAMPLE Viruses, worms, trojans.

[SOURCE: ISO/IEC 27032:2023, 3.15]

3.15
personally identifiable information
PII
information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.17). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2024, 3.7]

3.16
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.15) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others (e.g. PII processors (3.18)) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2024, 3.8]

3.17
PII principal
data principal
natural person to whom the *personally identifiable information (PII)* (3.15) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2024, 3.27]

3.18
PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.15) on behalf of and in accordance with the instructions of a *PII controller* (3.16)

[SOURCE: ISO/IEC 29100:2024, 3.10]

3.19
privacy data sharing agreement
clauses for privacy protection in a data sharing agreement

Note 1 to entry: A privacy data sharing agreement can involve data transfer, data processing, and sharing of *personally identifiable information (PII)* (3.15) between *joint PII controllers* (3.11).

[SOURCE: ISO/IEC TS 27570:2021, 3.22]

3.20
re-identification
process of associating data in a *de-identified dataset* (3.7) with the original *data principal* (3.17)

Note 1 to entry: A process that establishes the presence of a particular data principal in a dataset is included in this definition.

[SOURCE: ISO/IEC 20889:2018, 3.32]

3.21
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3) , or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

[SOURCE: ISO/IEC 27000:2018, 3.61]

3.22
strong authentication
authentication procedure using a minimum of two independent (from the security point of view) authentication mechanisms, with at least one of them being dynamic

[SOURCE: ISO 12812-1:2017, 3.57]

3.23
user profiling
activity to retrieve a set of attributes used by the system that are unique to a specific user/user group

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

AI	artificial intelligence
AML	anti-money laundry
API	application programming interface
ICT	Information and Communication Technology
KYC	know your customer
ML	machine learning
PII	personally identifiable information

5 Stakeholders and general considerations for fintech services

5.1 Stakeholders and business models for fintech services

Figure 1 illustrates the business model of fintech services. To provide fintech services, there are five entities involved: customers, fintech service providers as PII controller/joint PII controller, fintech service providers as PII processor, financial companies and regulators.

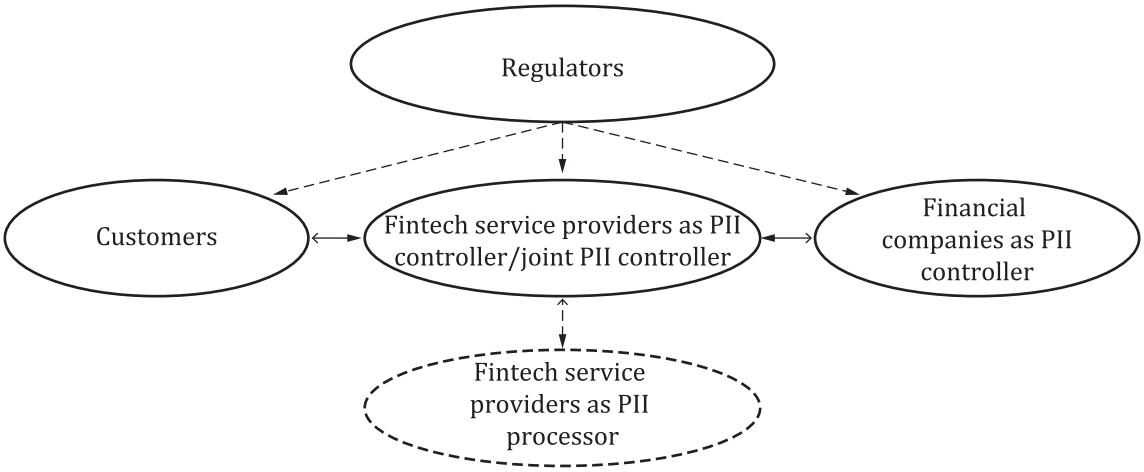

Figure 1 — Stakeholders for fintech services

Fintech service providers include all entities which provide fintech services to customers. It includes both so-called traditional financial services providers (i.e. banks, savings institutions, credit unions and other chartered financial institutions) and other entities, which can include eMoney operators, postal authorities and a variety of different commercial providers. These other entities are collectively referred to here as "non-bank providers". Annex C provides an example of architecture with an open platform for fintech service providers, as described in ITU-T X.1149.

Examples of business models in fintech services include:

— payment gateways;

— digital wallets;

— digital insurance;

— digital lending;

— peer-to-peer (P2P) lending;

— point of sale;

— payment banks;

— neo banking;

— alternative insurance underwriting;

— wealthtech;

— API-based bank-as-a-service platforms;

— personal finance;

— blockchain-based fintech services;

— equity crowdfunding;