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)

COPYRIGHT PROTECTED DOCUMENT

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.

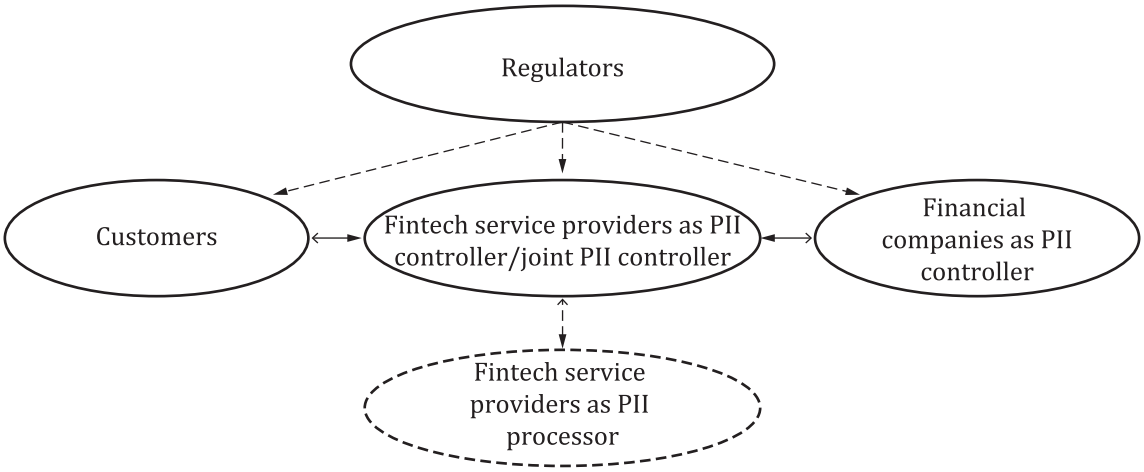


Figure 1 — Stakeholders for fintech services

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;

— project financing;

— microfinancing;

— financial agents;

— property investment management;

— claim service handling;

— credit scoring;

— e-KYC;

— online distress solution;

— market comparison.

Annex D provides the use cases for fintech services. Annex F provides the characteristics of AI-related PII processing for fintech services.

5.2 General considerations

5.2.1 General

Users of fintech services and applications should consider the points listed in 5.2.2 to 5.2.5.

5.2.2 Consumers

— Most consumers use at least one fintech application.

— Most consumers are concerned about data privacy and data sharing. Consumers' concerns about privacy extend to practically all types of financial and personally identifiable information (e.g. payment information, financial history, bank account user name and password, social security numbers, facial photo, digital copies of valid IDs). Annex A gives information on the purposes of collecting and processing PII.

— Consumers want to be able to control access to, and usage of, their information.

— Most fintech app users want to understand and be able to control how their data are accessed, collected, used and shared by third parties, but consumers are often not aware of fintech data aggregation practices.

— AI/ML technologies can be used to profile customers.

5.2.3 Regulators

— A data protection authority or privacy regulator serves as the body that implements and monitors data privacy regulation in a jurisdiction. Since fintech services process a vast amount of PII, the requirements set by each data protection authority should be addressed by the service providers.

— AML (anti-money laundering) compliance by regulation requires the collection, processing, and use of PII as part of customer due diligence (e.g. KYC); 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). See Annex B for examples of international and regional regulations related to anti-money laundering and fraud detection systems.

— Regulations on data privacy, data transfer, and data storage in processing PII can apply.

5.2.4 Service providers

— Various use cases are used to provide fintech services.

— Fraud detection by institutions also requires transaction and behavioural monitoring.

— Privacy issues are considered from both customer and back-office processing perspectives.

5.2.5 Financial company

— Financial companies, which include but are not limited to, banks, credit card issuers and payment gateways, are viewed by some as a trusted provider of data security and as a holder of what is considered sensitive data, so financial companies are expected to safeguard their customers' personal data.

— Financial companies can act as a system function provider that provides a financial-grade API.

6 General principles applicable to fintech services

When providing fintech services to customers, organizations should follow the privacy principles derived from ISO/IEC 29100:

— consent and choice;

— purpose legitimacy and specification;

— collection limitation;

— data minimization;

— use, retention and disclosure limitation;

— accuracy and quality;

— openness, transparency and access;

— individual participation and access;

— accountability;

— information security; and

— privacy compliance.

7 Actors in fintech services

7.1 Service providers as a PII controller

7.1.1 General

The role of the fintech service provider is categorized as either a PII controller or a PII processor. A service provider is considered a PII controller/joint PII controller when it controls and determines the processing of PII. It has the task of determining the purpose and the means of PII processing for its provided fintech services and identifying the appropriate privacy and security controls based on different conditions such as legal, business, contractual, and industry requirements.

7.1.2 Adherence to the privacy principles

As a PII controller, a service provider controls and decides on the PII processing and is responsible for the protection of PII. Depending on legal, business, contractual, and industry requirements these can be the common obligations of a PII controller.

PII controllers should ensure that the privacy principles described in ISO/IEC 29100 are adhered to during the implementation of fintech services.

In particular, if processing personal data legally requires consent from the user, the PII controllers as service providers implement the consent management function, which is a system or process for allowing customers to determine what PII data they are willing to share with service providers.

7.2 Service providers as a PII processor

A PII processor processes PII on behalf of or upon the instruction of the PII controller. The role of a PII processor can vary in every fintech service. For example, a PII controller that provides and maintains a lending application can task an organization as its PII processor in terms of handling the digital identity verification and credentials of the individuals who are applying for loans.

7.3 Customer as a PII principal

In most cases, every customer is considered a PII principal, since fintech services require their customer to provide PII for identity verification to avail their user-centric financial services.

Customers refers to all users of fintech service, i.e. individuals, merchants, billers and other payments acceptors; businesses; governments; and non-profit agencies. These groups can be collectively thought of as a customer of fintech services.

7.4 Financial company as a PII controller

A financial company is an entity engaged in the business of dealing with financial and monetary transactions such as deposits, loans, investments, and currency exchange. Financial companies encompass a broad range of business operations within the financial services sector including banks, trust companies, insurance companies, brokerage firms, and investment dealers.

7.5 Regulators

Where regulators develop and enforce a legal framework to monitor and oversee fintech activities, they should comprehensively document the policy and ensure that financial, consumer, antitrust, regulatory, cybersecurity, data protection and human rights bodies are notified thereof. This policy should be guided by best practices and relevant international standards.

In addition, regulators should document the data protection policy with adequate and coordinated levels of enforcement, addressing the financial sector and regulating cross-border data transfers to ensure equivalent and adequate levels of protection.

8 Privacy risks to actors

8.1 General privacy threats

General privacy threats can be grouped into seven threat categories:

— Linkability: a bad actor can establish the link between two or more actions, identities, and pieces of information, even if bad actors have no knowledge of the subject's identity.

— Identifiability: a bad actor can establish the link between an identity and an action or a set of data.

— Non-repudiation: the PII principal cannot deny having performed an action that other parties can neither confirm nor contradict.

— Detectability: a bad actor can detect a PII principal and distinguish whether an item of interest about that subject exists.

— Disclosure of information: a bad actor can disclose the data content or controlled release of data content.

— Unawareness: PII principals are unaware of their PII being collected and processed.

— Non-compliance: the personal data processing does not comply with relevant laws and/or policies.

There is a risk to the providers of fintech services that more information is required to be collected and stored than is necessary or safe. General privacy risks are as follows:

— Fintech services can leverage web-based service models and APIs. APIs can increase the exposure risks and induce vulnerability leading to potential data breaches, fraud, or misuse. This vulnerability can allow attackers to gain access to PII and sensitive data or execute other malicious actions such as data exfiltration, account takeover (ATO) and service disruption. Annex E provides a non-exhaustive list of common vulnerabilities and privacy risks related web-based applications.

— Cloud computing is widely accepted and implemented in the fintech services sectors, as the demand for faster computing and higher cost-efficiency grows. Cloud services are available on-demand, scalable to the customer needs, and delivered over the internet, thus availing local and global market outreach. While the use of cloud services offer access to next-generation computing performance levels at reasonable cost structures, this setup introduces new threats due to outsourcing workloads, cross-border processing and data storage. This poses potential legal and geo-political risks. In addition, unanticipated communications between Virtual Machines (VMs) can result in unpredictable and emerging vulnerabilities.

— Blockchain technologies can be leveraged for financial use cases, which have characteristics of "immutability" of the decentralized ledger/data storage implementation and can eliminate a single point of failure. Ensuring privacy while using blockchain technology is virtually impossible. Special attention should be paid when implementing the right to be forgotten, i.e. right of PII principal.

Possible organizational impacts in case of a privacy breach include:

— loss of reputation/goodwill;

— loss of strategic advantage to a competitor;

— breach of contractual obligation;

— failure to comply with all applicable legislation or regulations;

— economic losses due to compensation claims from individuals;

— economic losses due to project/system redesign;

— economic losses due to project/system failure;

— economic losses due to security measures, retrofitted after project launch.

It is recommended to identify the possible privacy risks of fintech services and their potential impact on the PII principals. In addition, it is also recommended to identify risk management and consequences of adverse privacy impacts on individuals that greatly affect the organization.

NOTE 1 Further guidance on conducting a privacy impact assessment (PIA) can be found in ISO/IEC 29134.

NOTE 2 Further guidance on organizational privacy risk management can be found in ISO/IEC 27557.

8.2 Privacy risks to service providers as PII controllers

Privacy risk is defined as the potential loss of control over personal information by the service provider. The following privacy risks for fintech services apply: unauthorized access, breaches, loss, manipulation, falsification, destruction or unauthorized disclosure to all collected data.

In general, privacy risks are any accidental or unlawful destruction; loss, alteration; unauthorized disclosure of, or access to, personal data as arising from data breach; data exposure on the operator side; lacking breach response; inadequate personal data disposal; lack of transparency in privacy policies; terms and conditions; collection of unnecessary data; personal data sharing; incorrect or outdated personal data and data transfer over insecure channels.

Typical risks to PII of organizations can include:

— Illegitimate access to PII – For example, PII are seen by an unauthorized person, even though this person does not use them. PII are copied and saved to another location without being used further. PII are disseminated more than necessary and beyond the control of the PII principals (e.g. unwanted dissemination of a photo over the internet, loss of control over information published in a social network). PII are used for purposes other than those planned and/or in an unfair manner (e.g. commercial purposes, identity theft, use against data principals) or correlated with other information relating to PII principals (e.g. correlation of residence address and real-time geolocation data).

— Manipulation of PII – For example, PII can be modified into invalid data, which cannot be used correctly, and the processing of modified PII can cause errors, malfunctions, or no longer provide the expected service (e.g. impairing the proper progress of important steps).

— Loss of PII – For example, PII is missing from personal data during processing, which generates errors, malfunctions, or provides a different service than the one expected (e.g. some allergies are no longer reported in a medical record, some information contained in tax returns has disappeared, which prevents the calculation of the tax amount). This missing PII can also sabotage the expected service (e.g. slowing down or blocking of administrative or commercial processes, inability to provide care due to the loss of medical records, inability of data principals to exercise their rights, etc.).

The following privacy risks to service providers as PII controllers should be considered:

— privacy breach of the general privacy principles described in Clause 6;

— data breaches/leakage: unintentional or deliberate compromise or revealing of information, to an unauthorized party;

— data disclosure and modification from inappropriate security measures;

— insufficient due diligence: lack of proactive actions;

— insufficient data breach response;

— platform/technology unreliability or vulnerability: platform/technology unreliability or vulnerability that causes or facilitates loss, inconvenience, or other harms;

— use of automated algorithmic scoring in fintech that can lead to discrimination;

— groundless PII transfer between jurisdictions;

— failure to comply with legal, regulatory and business obligations to customers. The examples include PII leakage notice to customer in a certain time of period;

— malware infection through open API of the fintech service, which leads to data leakage or data unavailability;

— insufficient logging and monitoring that allows attackers to penetrate systems further, maintain persistence, and tamper, extract or destroy data;

— IT system failures (caused by hacking, ransomware attack, etc.);

— automated decision making without consent;

— user profiling without authority that results in automatic decision;

— black-box, non-transparent AI-based automated decisions;

— use of weak customer authentication;

— re-identification when the de-identified dataset is linked with other external information;

— data breaches due to insufficient security of API.

8.3 Privacy risks to service providers as PII processors

The following privacy risks to service providers as PII processors should be considered:

— privacy breach of the general privacy principles described in Clause 6;

— breach of contract related to privacy with the PII controller;

— data breaches/leakage: unintentional or deliberate compromise or revealing of information, to an unauthorized party;

— data disclosure and modification from inappropriate security measures such as account hijacking, insecure application programming interfaces and malicious insiders;

— insufficient due diligence: lack of proactive actions;

— insufficient data breach response.

8.4 Privacy risks to customers as PII principals

The following privacy risks to customers as PII principals should be considered:

— inability of customers to access and modify data: customers do not have the ability to access, change or delete data related to them;

— inability to conduct customer's right for individual participation and access;

— insufficient due diligence: lack of proactive actions;

— physical damage;

— material damage;

— non-material damage;

— identity theft or fraud;

— financial loss;

— damage to reputation;

— insiders' risk to the customer, such as sharing intrusive information and unauthorized sharing with branches;

— sensitive PII exposure;

— identity exposure and corruption of PII;

— re-identification of datasets;

— exclusion or discrimination against individuals;

— revealing characteristics such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

— tracking or surveillance of the individual;

— systematic and extensive profiling;

— individuals denied services;

— PII processing regardless of whether fintech users are actually customers or prospective customers of fintech entities;

— lack of awareness or understanding regarding how and which data about the customer is collected or used, in cases where the customer is not familiar with the commonly used approaches of notifications for requesting consent.

8.5 Privacy risks to financial companies as PII controllers

The following privacy risks to financial companies as PII controllers should be considered:

— privacy breach of the general privacy principles described in Clause 6;

— inappropriate processing of PII transferred to third parties;

— lack of or insufficient record of disclosures of PII to third parties;

— inappropriate transfer without legal basis of PII to third parties;

— data breaches due to insufficient identity proofing;

— data breaches due to insufficient security of API.

9 Privacy controls for actors

9.1 General

An explicit scoping and understanding of financial business processes is a critical task for formulating secure data flows and limiting the user scope. Online risks can be caused by the participation of unknown, untrusted, or unexpected data users.

Data can be intercepted throughout the whole data flow. A robust implementation of cryptography and proper key management should be in place, so that data can be made intelligible, only to authorized parties.

The convenience of interlinking and automated retrieval, extraction and any processing among various entities or third parties, are some of the major privacy risks in fintech. Processes should have a strong integrated privacy framework in place, i.e. consent and choice, collection limitation and data minimization.

Since financial transactions and the customer's privacy require a higher degree of data protection, one way to protect these is to use attribute-based access controls. ISO/IEC 27551 provides a framework and establishes requirements for attribute-based unlinkable entity authentication.

Proper implementation of financial-grade APIs[37] and the derivative of unique identifiers of PII principals, i.e. tokens, can help reduce the exposure of actual personal information and risks of a data breach.

Another general privacy issue is the excessive permissions required by mobile applications. Fintech apps should be transparent and sufficiently explain to PII principals why it is necessary to access mobile phone cameras for biometric liveness detection and spoof detection, for the purposes of KYC. In addition, the transparency for permissions should be provided.

Mobile financial services highly rely on the use of mobile devices and networks. Cyber risks attached to distributed networking systems should be addressed, like monitoring communications and hacking cloud storage.

New technologies can bring unanticipated cyber risks, despite their intended purpose to introduce benefits. The challenges are generally attributed to technical vulnerabilities of new systems, uncertain business process designs, and high complexity of governance.

9.2 Privacy controls applicable to service providers as PII controllers

9.2.1 General

The controls specified in 9.2.2 to 9.2.18 should be implemented for the PII controller.

NOTE The term "organizations" in 9.2.2 to 9.2.18 refers to service providers as PII controllers.

9.2.2 Policies to ensure compliance with data protection regulations — Control

Organizations are expected to implement appropriate policies and adequate internal measures to ensure compliance with personal data protection regulations and, where relevant, respect consumers' right to personal data privacy. This can include, for example, verifying that mechanisms are in place to safeguard people's personal and financial information and verifying adequate security mechanisms to ensure that financial transactions are protected.

9.2.3 Request for permission and consent

9.2.3.1 Control for provision of permission

Where applicable, organizations should implement measures to ensure that requests for permission to collect, store and use personal data in relation to the expected purpose of the financial product or service are clear and understandable.

9.2.3.2 Control for provision of consent

Where applicable, organizations should implement measures to ensure that requests for permission to collect, store and use personal data are clear and the technical permissions required for the purpose are specified and bundled to the record of notice for the specified purpose.

Organizations should implement measures to ensure informed consent about their data at a relevant time and context.

For greater assurances, a notice required for the provision of electronic consent should be presented, with consistent vocabulary controls, recorded in a consistent formant. Interaction with a consent notice should be recorded as proof of notice, and a consent receipt provided to the individual as evidence of consent.

Requests for consent should avoid the use of language or terminology of an overly legal, technical or specialized nature. Consent should be freely provisioned, and a record of notice be kept, and a consent receipt provided, for digital evidence of the provisioned consent.

9.2.3.3 Control for periodic notices/consent

Periodic notice and consent should be implemented to exercise choice easily, since many customers have accounts for long periods of time and what they consented to in account opening stage can have been forgotten or no longer relevant.

NOTE See ISO/IEC 29184 for good practices on consent and notice.

9.2.4 Legitimate purpose — Control

Organizations should implement measures to use data only for legitimate purposes, including anti-money laundering and fraud detection, and in a manner that serves customers' interests. For example, this can be done via a legitimate purposes test, which limits the use of data to what is compatible, consistent, and beneficial to consumers, while allowing firms to use de-identified data to develop new and innovative products and services; and/or via a fiduciary duty requirement, which requires data collection and processing firms to always act in the interests of, and not in ways detrimental to, the subjects of the data.

9.2.5 Authentication mechanisms — Control

Organizations should use strong authentication mechanisms for services that hold confidential data, or for high value transactions. Strong authentication is used for:

— making service providers easier and safer to use; and

— protecting consumers against fraud, abuse, and other identity problems.

9.2.6 Automated decision making — Control

Organizations should put measures in place to ensure automated decisions are not made without consent.

Organizations should put measures in place so that user profiling cannot be created without authority, which can result in an automatic decision.

PII principals should be informed regarding automated decisions and the organizations should put in place human oversight, in particular when ML algorithms are adopted.

9.2.7 De-identification method — Control

Organizations should use strong de-identification techniques that allows identified data to be transformed into a de-identified dataset when designing innovative products and services.

Organizations should implement appropriate policy and adequate internal measures.

Organizations can use the privacy enhancing data de-identification techniques described in ISO/IEC 20889.

9.2.8 Risk management and governance arrangements — Control

Organizations should put in place adequate risk management and governance arrangements, comply with targeted risk management and operational reliability requirements, including for technology-related risks and outsourcing, and have specific competence in relation to matters such as information technology related risks.

Organizations should conduct the privacy impact assessment described in ISO/IEC 29134, which is integrated into the risk management to identify the possible privacy risks and their potential impact on the PII Principal.

9.2.9 Preventing algorithmic discrimination — Control

Organizations should implement measures to apply anti-discrimination rules to algorithms, follow appropriate procedures, controls, and safeguards during development, testing, and deployment, to conduct regular external auditing of algorithmic systems and to provide consumers with the right to not be subject solely to automatic processing and the right to request human intervention.

9.2.10 Policy of encryption — Control

Organizations should establish and implement the policy of encryption to protect sensitive data when storing and transmitting sensitive information such as usernames, passwords, credit card numbers and sensitive documents. In addition, organizations should generate and use cryptographic keys used for encryption according to their intended use, manage safely them to avoid exposure, and not store them in plaintext or put them by use of hard-coding inside the program of the system.

9.2.11 PII transfers between jurisdictions — Control

Organizations should inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer can object to such changes or terminate the contract.

9.2.12 Malware infection — Control

Organizations should prevent, detect and respond to malware infection through appropriate controls including security patches, limiting access to suspicious websites, logging and data backups.

9.2.13 Data breach notification to the supervisory authority — Control

Organizations should provide mechanisms to notify the supervisory authority of any data breaches and the customers affected.

9.2.14 Security logging and monitoring policy — Control

Organizations should establish a security logging and monitoring policy and implement processes such as preserving the required logs for a certain period of time and reviewing them periodically, to support forensic investigations around potential or realized breaches.

For example, whenever a bank's staff queries the bank balance of a consumer, organizations should log a brief justification in the bank system, which can be audited periodically.

9.2.15 Recovery procedures — Control

Organizations should establish recovery procedures to enable recovery against failures caused by IT system failures (caused by hacking, ransomware attack, etc.).

9.2.16 Backup policy — Control

When establishing a backup policy, organizations should consider which critical data and systems require protection, the frequency of both full and incremental backups, retention period and maintaining the backup records and backup data for a certain period of time.

9.2.17 Data provenance and traceability — Control

Organizations should keep track of the lifecycle of personal/sensitive data to ensure that they are not tampered with or subject to incidents such as data breaches.

9.2.18 Explainable and analysable automatic decision — Control

Organizations should operate an explainable and analysable automated decision that helps them to understand and interpret predictions made by machine learning models.

9.3 Privacy controls applicable to service providers as PII processors

9.3.1 General

In addition to the guidance in ISO/IEC 27002 and ISO/IEC 27701 for service providers as PII processors, the controls in 9.3.2 to 9.3.7 should be implemented.

NOTE The term "organizations" in 9.3.2 to 9.3.7 refers to service providers as PII processors.

9.3.2 Contract agreement — Control

Organizations should put measures in place to avoid breaches of contract. Such measures should be authorized by the PII controller to ensure that the contract on processing PII addresses the organization's role in aiding with the PII controller's obligation.

NOTE Legal requirements can apply.

9.3.3 Non-disclosure — Control

Organizations should put measures in place to avoid unintentional or deliberate compromise or revealing of information to an unauthorized party.

9.3.4 Improper data disclosure — Control

Organizations should put appropriate security measures in place to avoid improper data disclosure and modification from risks such as account hijacking, insecure application programming interfaces and malicious insiders, and to ensure data availability.

For example, organizations should implement appropriate security measures to avoid unauthorized data sharing with a loan collection agent or third-party loan agent.

9.3.5 Risk assessment — Control

Organizations should implement appropriate security measures to pay due diligence so that sufficient proactive actions are taken based on risk assessment.

9.3.6 Personal data breach management — Control

Organizations should establish procedures for the identification and recording of breaches of PII. Additionally, organizations should establish responsibilities and procedures related to notifying relevant parties of PII breaches (including the timing of such notifications) and the disclosure to authorities, taking into account the applicable legislation and regulations.

9.3.7 Privacy Impact Assessment (PIA) — Control

Organizations should use the privacy impact assessment described in ISO/IEC 29134 to identify the privacy risks and impacts thereof.

9.4 Privacy controls by fintech service providers for customers as PII principals

9.4.1 General

The controls specified in 9.4.2 to 9.4.10 should be implemented by service providers for the PII principal.

NOTE The term "organizations" in 9.4.2 to 9.4.10 refers to fintech service providers for customers as PII principals.

9.4.2 Rights of PII principals — Control

Service providers should provide customers with mechanisms to obtain access to, correct and erase their PII, if requested, and without undue delay.

Service providers should provide customers with mechanisms to access their right for individual participation and access.

9.4.3 Due diligence — Control

Service providers should provide customers with mechanisms to pay due diligence to take proactive actions against attacks.

9.4.4 PII management— Control

Service providers should provide customers with mechanisms to prevent unauthorized exposure to sensitive PII of customers' device.

Service providers should provide customers with mechanisms to prevent corruption of PII through the customers' devices.

9.4.5 Re-identification and anonymization — Control

Organizations should implement procedures and mechanisms to prevent re-identification from deidentified datasets and re-identification from anonymized datasets.

9.4.6 Discrimination — Control

Organizations should implement procedures and mechanisms to prevent revealing the characteristics of PII, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.

9.4.7 Surveillance — Control

Organizations should implement procedures and mechanisms to prevent tracking or surveillance of the individual from dataset of customers.

9.4.8 Systematic and extensive profiling — Control

Organizations should implement procedures and mechanisms to prevent systematic and extensive profiling from dataset of customers.

9.4.9 Accessible information — Control

Customers should be provided with clear and easily accessible information related to the fintech services and the processing of their PII. Where appropriate, the information should be given at the time of PII collection and PII sharing with other PII controllers/processors.

9.4.10 PII processing after log-in — Control

Only the PII of customers should be collected and processed after customers have logged onto PII processing systems.

9.5 Privacy controls applicable to financial companies as PII controllers

9.5.1 General

The controls specified in 9.5.2 to 9.5.4 should be implemented for PII controllers.

NOTE The term "organizations" in 9.5.2 to 9.5.4 refers to financial companies as PII controllers.

9.5.2 Processing limitation — Control

Organizations should limit the processing of PII to that which is adequate, relevant, and necessary for the identified purposes.

9.5.3 PII disclosure limitation — Control

If applicable, organizations should record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.

9.5.4 PII transfer management — Control

Organizations should identify and document the relevant basis for any transfer of a customer's PII to other PII controllers.

10 Privacy guidelines for actors

10.1 Privacy risk treatment

This clause provides privacy guidelines focusing a set of privacy requirements for each actor.

A comprehensive strategy to mitigate data privacy risks is essential in organizational countermeasures. The essence of a data privacy risk mitigation can be derived through a well-planned and properly implemented privacy policy. The following steps should be considered to effectively implement a comprehensive policy to mitigate data privacy risks through organizational countermeasures, including staff training on security and privacy and appropriate data usage:

1. Identifying and classifying sensitive information assets.
2. Implementing monitoring of information accessibility, and identity and access management functions.
3. Protecting information through a variety of security controls and technologies such as encryption, tokenization, de-identification, as applicable for data in motion and data at rest.
4. Having a clear data disposal policy in place.
5. Planning for a data breach, i.e. a security or disaster event, by implementing a proper business continuity and disaster recovery plan (BC/DR), which is tested annually.

10.2 Service providers as PII controllers

The following privacy guidelines apply to PII controllers:

NOTE Legal requirements can apply.

— Processing: Organizations should not access, use or process data on behalf of the customer except as otherwise required to deliver the services and to provide relevant technical support, maintenance and improvement.

— Data access, modification and deletion: When the customer's personal data are uploaded while using the services, the PII principal may access, modify or delete data by logging into the services using common protocols and tools. Modification and deleting requests may also be made available to customer account's fraud specialist, via a support ticket, or other written notice. Upon termination or expiry of the services and upon written request by the customer, all customer personal data in its possession or control will be deleted.

— Cooperation and PII principals' rights: Organizations should provide reasonable and timely assistance to customer according to a privacy data sharing agreement and the services, to enable the customer to respond to a request from a PII principal to exercise any of its rights (including rights of access, correction, objection, erasure and data portability, as permitted), and any other correspondence, enquiry or complaint received from a PII principal, regulator or third party in connection with the processing of the personal data.

— Privacy impact assessment: Organizations should provide the customer with reasonable assistance in support of a data protection impact assessment, solely in relation to customer personal data, the privacy data sharing agreement, the services and where the customer would not otherwise have access to the relevant information.

— Confidentiality: It is expected that organizations implement measures to ensure appropriate contractual obligations related to confidentiality with its personnel and that these survive the termination of the engagement.

— Security: Organizations should ensure that appropriate technical and organizational safeguards exist for the processing of personal data including the hiring of qualified personnel, physical data centre access controls, systems access controls, data access controls, data transmission protocols, systems logging and backup systems.

10.3 Service providers as PII processors

All relevant legislative statutory, regulatory, and contractual requirements should be explicitly identified, documented and kept up to date. The contract between the organization and the subcontractor should include provisions on privacy by design and privacy by default, notification of breaches involving PII to a regulator, notification of breaches involving PII to PII principals, and the assurance of assistance by the organization if prior consultations with relevant PII protection authorities are needed.

10.4 Customers as PII principals

Customers should have meaningful access to, and control of, their PII, including data mined from the data collected or derived from the profiles that have been generated by third parties, and information about how it was obtained. Consent should be informed, meaningful, and granular enough to control different possible uses of the customer's PII. Their data should be used to empower them, not to justify exclusionary practices or surveillance schemes. Customers should be given the ability to make decisions about their PII at relevant times and in relevant contexts.

Consumers should be aware of the necessary knowledge and skills to understand how their PII is used and to fully exercise their consumer rights in this domain. Consumers should be aware of the increasing risks to the integrity of their personal data and their privacy.

10.5 Financial companies as PII controllers

Organizations should take measures to ensure customer’s PII be protected when using any AI based automatic decision-making process.

Organizations as financial companies should undertake in-depth privacy assessments, prior to the deployment of fintech within their programmes and projects that:

— address the needs of individuals concerned;

— include a gender analysis to identify the gender and an assessment of the gender impacts to facilitate understanding and map the ways in which different genders are affected by the fintech services;

— address the unexpected consequences that arise from the implementation of fintech.

Organizations should develop mitigation strategies for the risks identified in this assessment process.

Annex A
(informative)

Purpose of collecting and processing PII

A.1 General

The first and primary reason for collecting and processing PII in a fintech context is to deliver a core financial service. This includes user facilitation, statistical collection, and other regulatory collection, e.g. national ID infrastructure, tax (unless this is part of the service delivery).

Two other major purposes include:

a) Anti-money laundering. This refers to a set of laws, regulations and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income. Although anti-money-laundering (AML) laws cover a relatively limited range of transactions and criminal behaviours, their implications are far-reaching. AML compliance officers are often appointed to oversee anti-money laundering policies and ensure that banks and other financial institutions are compliant.

b) Fraud detection. This is a set of activities undertaken to prevent money or property from being obtained through false presences. Fraud detection is applied to many industries such as banking or insurance. In banking, fraud can include forging checks or using stolen credit cards. Other forms of fraud can involve exaggerating losses or causing an accident with the sole intent for the pay-out.

A.2 PII collected by a fraud detection system

Table A.1 provides examples an non-exhaustive list of PII which can be collected by a fraud detection system (FDS).[4]

NOTE Whether the entities are permitted to collect PII data depends on the fraud detection purpose, considering the principles in ISO/IEC 29100.

Table A.1 — Examples of PII collected by fraud detection

Category	PII items
Data for identifying customers	— Name — Address — Date of birth — National/local identifiers (National ID, social security number, driver's license number, health ID, etc.)
Data for communication protocols	— IP (Internet Protocol) — Virtual Privacy Network (VPN) IP — MAC address
Data for system	— Name, manufacturer, version and language of the operation system — Name, manufacturer, version and language of the browser used — Model name, serial number of hardware disc — Model name, serial number of mother board — Type or identifier of CPU (central processing unit) — Security status code from the anti-virus program or keying protection program — Identification code of the virtual operation system
Other data	— Account numbers — Biometrics (for account opening: biometric/facial liveness test and spoof detection) — Transaction history (which can include time and location)

Annex B
(informative)

Examples of international and regional regulations

B.1 The Financial Action Task Force

The Financial Action Task Force (FATF) provides an example of how legal entities can conduct know your customer (KYC) ID verification, by requesting and verifying the customer's proof of identity (e.g. using a passport).[28]

FATF's Guidance on Anti-Money Laundering (AML) and Combating the Financing Of Terrorism (CFT) promotes the use of simplified customer due diligence measures such as electronic identity verification, while appropriately mitigating the ML/TF (money laundering and terrorist financing) risks. [42] The FATF Guidance document recommends that:

— all records of high-risk customers be kept for a duration of five years. If a company fails to keep these records within the mandatory time period, companies can face applicable fines.

— accounts be regularly monitored for suspicious activities by checking if transactions exceed an established threshold, also if reasons behind said transactions are inconclusive.

— suspicious activity be reported to the appropriate financial intelligence unit, if there are reasonable grounds that these activities are related to money laundering and terrorist financing.

— a range of effective sanctions be applied, including fines, to deal with legal persons and obliged entities that fail to comply with AML/CFT requirements.

B.2 The United States' Bank Secrecy Act (BSA) and the USA Patriot Act

The United States' Bank Secrecy Act (BSA) and USA Patriot Act are examples of regulations related to money laundering. These regulations specify the following.

— Under the BSA,[43] banks and other financial institutions are required to file reports of cash transactions, currency transactions (CTR) and International Transportation of Currency or Monetary Instruments (CMIRs) in the sum of USD 10 000 or more. This sum may be attained in a single transaction or a series of transactions that appear to be connected.

— Section 352 of the USA Patriot Act[44] requires financial institutions to establish AML compliance programmes, which must include: the development of internal controls; designation of an AML compliance officer; an ongoing employee training program; and scheduled independent audits.

— The US Department of Justice may bring criminal actions for money laundering that can include fines, imprisonment and forfeiture actions.

— Any individual, including a bank employee, intentionally violating the BSA or its implementing regulations, is subject to a criminal fine of up to USD 250,000 or five years in prison, or both.

— A bank that violates certain BSA provisions faces criminal money penalties up to USD 1 million, or twice the value of the transaction.

— Legal entities are required keep records of all cash transactions and inform the Financial Crimes Enforcement Network (FinCEN) of transactions that are linked to money laundering and terrorist financing.

In a bid to decrease the success rates of financial crimes, the BSA mandates financial institutions to make monetary instrument logs (MLIs) for cash purchases of monetary instruments with a total value of USD 3 000 to USD 10 000.

B.3 European Union – Fourth and Fifth Anti-Money Laundering Directives (AMLD4 and AMLD5)

The fourth and fifth Anti-Money Laundering Directives (AMLD4 and AMLD5)[45] in the European Union provide another example of regulations related to money laundering.

The anti-money laundering directives aim to prevent the money laundering and terrorist financing within the European financing system. These directives are valid for all legal entities operating in the European Union.

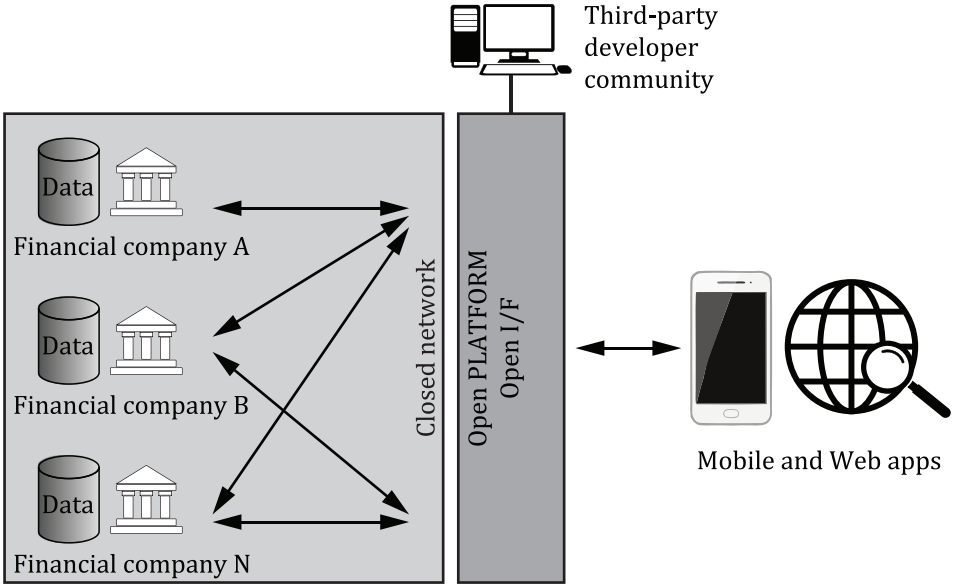
AMLD4 allows companies to employ electronic identity verification or e-KYC to verify customers remotely. This can be done through a selfie-based ID verification or video-based ID verification.

Annex C
(informative)

Example of open platform architecture for fintech service providers

Figure C.1 shows an example of architecture with emerged fintech service providers, which are not in the architecture of traditional digital financial services. Financial companies hire different fintech companies to develop diverse service apps and provide respective APIs for them. This architecture allows a financial company to provide users with respective apps for each of its services.

This architecture has limited data sharing, meaning that the data of a financial company is opened to a fintech company so that the fintech company has a dedicated authorization to access a user's data in this financial company, but the fintech company is not authorized to access data of the same user in other financial companies. Whenever the fintech company accesses the user's data beyond agreement with the origin financial company, it must obtain permission or authorization. From the user's view point, interfaces with different fintech companies are still different and not compatible. Fintech companies must secure each of its interfaces with each financial company and user.



Key

I/F interface

Figure C.1 — Example of open platform architecture for fintech service providers

Annex D
(informative)

Use cases for fintech services

D.1 Decentralized consent service

A key challenge to the finance industry is that it is only partially opened; banks have incumbent services which are required to be open and to provide people with consent-based access and delegation. However, this is not consent but a permitted authorization framework. In a decentralized consent system, the user can decide who gets access to user's data and for what purpose.

Some banks provide a data verification meta-vault and consent notary service(s). In this case, consent is utilized technically as a) a method of data flow and access control b) a tool for data governance interoperability. An old but vastly innovative technology is called a record and a receipt, where the concept of double ledger accounting is further extended to apply to consent as a digital currency. In this scenario, a principal provides a third-party digital service with a consent token, which is relayed as a verifiable credential to the digital-bank verification service. Consent receipts are portable as consent tokens and are stored in the vault as micro-consent credentials, used to allow the flow of data providing third-party access. The objective of bank service is to provide a pseudonymous service by default, which eliminates the need to identify and monitor individuals across all fintech services. Providers are permitted to collect, access and use specific data in a profile controlled by the PII principal. All access is logged in the digital-vault account; more advanced and highly assured systems are expected to be interoperable with the set of international standards on data governance, such as ISO/IEC 38500, which is used as a basis for open consent-based banking.

In this scenario of decentralized consent, the standardized digital privacy transparency is generated using the privacy framework specified in ISO/IEC 29100, the online notice and consent structure and controls specified in ISO/IEC 29184, and the notice and consent record information structure specified in ISO/IEC TS 27560, which are required for decentralized consent record management.

In such a standardized digital privacy context, consent and data controls can effectively be decentralized to the PII principal in the same way as receipts.

Furthermore, this record and receipt architecture can be utilized to address the additional challenges listed in Clause 8.

Data collected by the individual can be linked and should remain distributed among the data vault, personal devices, open profiles and third-party services. The records of processing can be put into the vault to be used as digital evidence of a company's treatment of personal data, notices, notifications and disclosures. Forensic tools for human understanding of digital and self-surveillance, or for collection of personal data from third parties can then be discovered.

Most importantly, using decentralized consent services means that it is no longer necessary for individuals to be identified by every service provider and that they can access privacy rights independently of service provider.

In this context, the bank is utilized as a consent verifier, ensuring a service where the user has the authority to issue the consent token and then to act as a relying party for the service to authenticate the individual authorizing access to personal identifiers and collecting metadata or consent to make a profile.

D.2 Fintech services using AI/ML

Artificial intelligence is used in a variety of fintech applications. A financial services customer frequently encounters fintech applications which are empowered by AI during everyday routines. Some examples are specified below.

— Biometric recognition using AI: Two factor authentication using a password, PIN or device with biometrics such as fingerprint and voice are used to access secure accounts. Artificial intelligence can improve the speed and accuracy of biometric recognition.

— Chatbot: Conversational applications such as chatbots are used for bank customers who prefer to ask for services rather than navigate fields and menus. Insurtech refers to technological innovations that are created and implemented to improve the efficiency of the insurance industry. Insurtech companies can use chatbots to deliver end to end insurance enquires with claims being paid in seconds.

— Customized service: Machine learning and artificial intelligence rely on large datasets. Banks have transactional data of customers gathered over many years, enabling them to offer targeted financial services using AI powered recommendation engines. Customer behavioural data can be used to predict the future needs of customers and offer them tailored services in real time, including advice on how to spend and save their money.

— Estimation of property damage: Computer vision AI applications can be used by insurance companies to automatically estimate property damage and repair costs from photographs.

— Personalised financial services: The user experience of leading B2C (business to customer) fintech platforms using AI offers simple, low friction interfaces, while ML algorithms work behind the scenes to deliver fast and personalised financial services. This growing ecosystem also includes companies that specialize in credit scoring, sentiment analysis and regulatory compliance.

— Edge computing: A lot of the heavy computation of AI can be done on the customer's device rather than the cloud. This reduces latency time with faster responses and deals with some of the security issues associated with sharing PII with third parties. Edge computing in 5G especially enhances the performance of mobile fintech applications that use machine learning and artificial intelligence.

Annex E
(informative)

List of common vulnerabilities and privacy risks

The following common vulnerabilities and privacy risks should be considered.

NOTE This list in not exhaustive.

— Web application vulnerabilities.

— Operator-sided data leakage: Failure to prevent the leakage of any information containing or related to user data, or the data itself, to any unauthorized party resulting in loss of data confidentiality. This can be introduced either due to an intentional malicious breach or an unintentional mistake e.g. caused by insufficient access management controls, insecure storage, duplication of data or a lack of awareness.

— Insufficient data breach response: Not informing the affected persons (PII principals) about a possible breach or data leak, resulting either from intentional or unintentional events; failure to remedy the situation by fixing the cause; not attempting to limit the leaks.

— Consent on everything: Aggregation or inappropriate use of consent to legitimate processing. Consent is “on everything” and not collected separately for each purpose (e.g. use of website and profiling for advertising).

— Non-transparent policies, terms and conditions: Not providing sufficient information to describe how data are processed, such as its collection, storage, and processing. Failure to make this information easily accessible and understandable.

— Insufficient deletion of user data: Failure to delete personal data effectively and punctually after termination of the specified purpose or upon request.

— Insufficient data quality: The use of outdated, incorrect or bogus user data. Failure to update or correct the data.

— Missing or insufficient session expiration.

— Inability of users to access and modify data: Users do not have the ability to access, change or delete data related to them.

— Collection of data not required for the user-consented purpose: Collecting descriptive, demographic or any other user-related data that are not needed for the purposes of the system. This applies also to data for which the user did not provide consent.

Annex F
(informative)

Characteristics of AI-related PII processing for fintech services

F.1 Processing of large data

A large amount of learning data are utilized during AI development, and it is highly likely that various kinds of PII and sensitive privacy data are included in it. Also, there are high demands for continuous utilization of such data during service operation.

It is important to collect PII in a legitimate way, e.g. ensuring PII principals' consent and pseudonymization, using PII within foreseeable and permitted purposes, and safely managing it.

F.2 Complexity and opacity

The PII processing method used in the development and operation an AI service is very complicated. As it is difficult for users to know how their PII is processed, PII principals' exercise of rights can be limited.

It is important to guarantee user participation by transparently disclosing the details of PII processing so that PII principals can exercise their rights in regard to the processing of their personal information.

F.3 Automation and uncertainty

In general, the AI model uses the knowledge and probability-based reasoning method to analyse and process data.

As it is difficult to predict the results of data processing when in the process of using it to develop and operate automated service data, problems such as privacy infringement, social discrimination and bias can arise.

To ensure that privacy is protected, it is important to responsibly manage PII processing and consider the fairness of the results of PII processing so that users are not discriminated.

Bibliography

[1] IPQualityScore, Data Processing Agreement, https://www.ipqualityscore.com/data-processing-agreement

[2] Eurofinas, FRAUD PREVENTION AND DATA PROTECTION A Eurofinas - ACCIS Report on Fighting Fraud in Consumer Lending

[3] ITU-T X.1157, *Technical capabilities of fraud detection and response for services with high assurance level requirements*

[4] Sohee Park, Jinhyeok Jang, & Daeseon Choi (2020). A Study on User Authentication Model Using Device Fingerprint Based on Web Standard. Journal of the Korea Institute of Information Security & Cryptology, 30(4), 631-646. Available at https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE09858939.

[5] ISO 12812-1:2017, *Core banking — Mobile financial services — Part 1: General framework*

[6] ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques*

[7] ISO/TR 23455:2019, *Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*

[8] ISO 21586, *Reference data for financial services — Specification for the description of banking products or services (BPoS)*

[9] ITU-T X.1149(2020), *Security framework of an open platform for FinTech services*

[10] EU, Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 1.0, Adopted on 17 July 2020

[11] ISO/IEC/IEEE 26531:2023, *Systems and software engineering — Content management for product life cycle, user and service management information for users*

[12] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[13] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

[14] ISO/IEC 27018:2019, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[15] ISO/IEC 27032:2023, *Cybersecurity — Guidelines for Internet security*

[16] ISO/IEC/TS 27560, *Privacy technologies — Consent record information structure*

[17] ISO/IEC/TS 27570:2021, *Privacy protection — Privacy guidelines for smart cities*

[18] ISO/IEC 27551:2021, *Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication*

[19] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[20] ISO/IEC 29100:2024, *Information technology — Security techniques — Privacy framework*

[21] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[22] ISO/IEC 29134:2023, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[23] ISO/IEC 29151:2017, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[24] ISO/IEC 38500:2024, *Information technology — Governance of IT for the organization*

[25] EU's Anti Money Laundering Directive 5

[26] ISO/IEC 29184:2020, *Information technology — Online privacy notices and consent*

[27] EU's Payment Services Directive 2 for Open Banking

[28] Financial Action Task Force at https://www.fatf-gafi.org/

[29] United States' Bank Secrecy Act (BSA) | USA Patriot Act

[30] ISO 20022, *Financial services — Universal financial industry message scheme*

[31] ISO 23234:2021, *Buildings and civil engineering works — Security — Planning of security measures in the built environment*

[32] ISO Guide 73:2009[1)], *Risk management — Vocabulary*

[33] ITU FIGI, Digital Financial Services security assurance framework

[34] ITU ITU-T Focus Group Digital Financial Services, The Digital Financial Services Ecosystem

[35] ITU-T Focus Group Digital Financial Services, Security Aspects of Digital Financial Services (DFS

[36] Marianthi Theoharidou, Nick Papanikolaou, Siani Pearson and Dimitris Gritzalis, "Privacy risks, security and accountability in the Cloud," IEEE Cloudcom-2013, 2013.

[37] OWASP Top 10 Privacy Risks available at https://owasp.org/www-project-top-10-privacy-risks/

[38] Personal Information Protection Commission (Korea). "Artificial Intelligence (AI) Personal Information Protection Self-Checklist", 31 May, 2021 (available at https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000842903&fileSn=0)

[39] Everyday fintech use cases for A.I. https://fintechcircle.com/insights/fintech-use-cases-for-ai/

[40] World Bank Group, Consumer Risks in Fintech - New Manifestations of Consumer Risks and Emerging Regulatory Approaches, April 2021.

[41] Open I.D. Financial-grade API Security Profile (FAPI) 1.0 – Part 1: Baseline – A secured OAuth profile that aims to provide specific implementation guidelines for security and interoperability, March 12, 2021 (available at https://openid.net/specs/openid-financial-api-part-1-1_0.html.

[42] FAYA. The FATF Recommendations, November 2023, available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

[43] The United States' Bank Secrecy Act (BSA). available at https://www2.occ.gov/

[44] Patriot U.S.A. Act, available at https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

[45] European Union, Anti-Money Laundering Directives, available at https://www.lseg.com/en/risk-intelligence/financial-crime-risk-management/eu-anti-money-laundering-directive

[46] ISO/IEC 27557:2022, *Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management*

1) Withdrawn.

ICS 35.030; 35.240.40; 03.060
Price based on 30 pages

iso.org