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/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **4**
5 Stakeholders and general considerations for fintech services **5**
5.1 Stakeholders and business models for fintech services 5
5.2 General considerations 6
5.2.1 General 6
5.2.2 Consumers 6
5.2.3 Regulators 6
5.2.4 Service providers 6
5.2.5 Financial company 7
6 General principles applicable to fintech services **7**
7 Actors in fintech services **7**
7.1 Service providers as a PII controller 7
7.1.1 General 7
7.1.2 Adherence to the privacy principles 7
7.2 Service providers as a PII processor 8
7.3 Customer as a PII principal 8
7.4 Financial company as a PII controller 8
7.5 Regulators 8
8 Privacy risks to actors **8**
8.1 General privacy threats 8
8.2 Privacy risks to service providers as PII controllers 9
8.3 Privacy risks to service providers as PII processors 11
8.4 Privacy risks to customers as PII principals 11
8.5 Privacy risks to financial companies as PII controllers 12
9 Privacy controls for actors **12**
9.1 General 12
9.2 Privacy controls applicable to service providers as PII controllers 13
9.2.1 General 13
9.2.2 Policies to ensure compliance with data protection regulations — Control 13
9.2.3 Request for permission and consent 13
9.2.4 Legitimate purpose — Control 13
9.2.5 Authentication mechanisms — Control 14
9.2.6 Automated decision making — Control 14
9.2.7 De-identification method — Control 14
9.2.8 Risk management and governance arrangements — Control 14
9.2.9 Preventing algorithmic discrimination — Control 14
9.2.10 Policy of encryption — Control 14
9.2.11 PII transfers between jurisdictions — Control 14
9.2.12 Malware infection — Control 15
9.2.13 Data breach notification to the supervisory authority — Control 15
9.2.14 Security logging and monitoring policy — Control 15
9.2.15 Recovery procedures — Control 15
9.2.16 Backup policy — Control 15
9.2.17 Data provenance and traceability — Control 15
9.2.18 Explainable and analysable automatic decision — Control 15
9.3 Privacy controls applicable to service providers as PII processors 15

© ISO/IEC 2024 – All rights reserved

9.3.1 General ... 15
9.3.2 Contract agreement — Control ... 15
9.3.3 Non-disclosure — Control ... 16
9.3.4 Improper data disclosure — Control ... 16
9.3.5 Risk assessment — Control ... 16
9.3.6 Personal data breach management — Control ... 16
9.3.7 Privacy Impact Assessment (PIA) — Control ... 16
9.4 Privacy controls by fintech service providers for customers as PII principals ... 16
9.4.1 General ... 16
9.4.2 Rights of PII principals — Control ... 16
9.4.3 Due diligence — Control ... 16
9.4.4 PII management— Control ... 16
9.4.5 Re-identification and anonymization — Control ... 17
9.4.6 Discrimination — Control ... 17
9.4.7 Surveillance — Control ... 17
9.4.8 Systematic and extensive profiling — Control ... 17
9.4.9 Accessible information — Control ... 17
9.4.10 PII processing after log-in — Control ... 17
9.5 Privacy controls applicable to financial companies as PII controllers ... 17
9.5.1 General ... 17
9.5.2 Processing limitation — Control ... 17
9.5.3 PII disclosure limitation — Control ... 17
9.5.4 PII transfer management — Control ... 17

10 Privacy guidelines for actors ... 18
10.1 Privacy risk treatment ... 18
10.2 Service providers as PII controllers ... 18
10.3 Service providers as PII processors ... 19
10.4 Customers as PII principals ... 19
10.5 Financial companies as PII controllers ... 19

Annex A (informative) **Purpose of collecting and processing PII ... 20**

Annex B (informative) **Examples of international and regional regulations ... 22**

Annex C (informative) **Example of open platform architecture for fintech service providers ... 24**

Annex D (informative) **Use cases for fintech services ... 25**

Annex E (informative) **List of common vulnerabilities and privacy risks ... 27**

Annex F (informative) **Characteristics of AI-related PII processing for fintech services ... 28**

Bibliography ... 29

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

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]

© ISO/IEC 2024 – All rights reserved