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.