

ISO/IEC 27562:2024-12 (E)

Information technology - Security techniques - Privacy guidelines for fintech services

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
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