

ISO/IEC 29100:2011-12 (E)

Information technology - Security techniques - Privacy framework

Contents		Page
Foreword		v
Introduction.....		vi
1 Scope		1
2 Terms and definitions		1
3 Symbols and abbreviated terms		4
4 Basic elements of the privacy framework.....		5
4.1 Overview of the privacy framework.....		5
4.2 Actors and roles		5
4.2.1 PII principals		5
4.2.2 PII controllers.....		5
4.2.3 PII processors.....		5
4.2.4 Third parties.....		6
4.3 Interactions		6
4.4 Recognizing PII.....		7
4.4.1 Identifiers		7
4.4.2 Other distinguishing characteristics.....		7
4.4.3 Information which is or might be linked to a PII principal		8
4.4.4 Pseudonymous data		9
4.4.5 Metadata		9
4.4.6 Unsolicited PII.....		9
4.4.7 Sensitive PII		9
4.5 Privacy safeguarding requirements		10
4.5.1 Legal and regulatory factors		11
4.5.2 Contractual factors.....		11
4.5.3 Business factors.....		12
4.5.4 Other factors		12
4.6 Privacy policies		13
4.7 Privacy controls.....		13
5 The privacy principles of ISO/IEC 29100.....		14
5.1 Overview of privacy principles		14
5.2 Consent and choice		14
5.3 Purpose legitimacy and specification		15
5.4 Collection limitation		15
5.5 Data minimization.....		16
5.6 Use, retention and disclosure limitation		16
5.7 Accuracy and quality		16
5.8 Openness, transparency and notice		17
5.9 Individual participation and access.....		17
5.10 Accountability.....		18
5.11 Information security		18
5.12 Privacy compliance.....		19
Annex A (informative) Correspondence between ISO/IEC 29100 concepts and ISO/IEC 27000 concepts		20
Bibliography.....		21

Figures

Figure 1 – Factors influencing privacy risk management 11

Tables

Table 1 – Possible flows of PII among the PII principal, PII controller, PII processor and a third party and their roles 7

Table 2 – Example of attributes that can be used to identify natural persons 8

Table 3 – The privacy principles of ISO/IEC 29100 14

Table A.1 – Matching ISO/IEC 29100 concepts to ISO/IEC 27000 concepts 20