DIN EN ISO/IEC 29100:2020-09 (E)

Information technology - Security techniques - Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018)

Contents

Page

European foreword 4

Foreword 5

Foreword 6

Introduction 7

1 Scope 8

2 Terms and definitions 8

3 Symbols and abbreviated terms 11

4 Basic elements of the privacy framework 12
4.1 Overview of the privacy framework 12
4.2 Actors and roles 12
4.2.1 PII principals 12
4.2.2 PII controllers 12
4.2.3 PII processors 12
4.2.4 Third parties 13
4.3 Interactions 13
4.4 Recognizing PII 14
4.4.1 Identifiers 14
4.4.2 Other distinguishing characteristics 14
4.4.3 Information which is or might be linked to a PII principal 15
4.4.4 Pseudonymous data 16
4.4.5 Metadata 16
4.4.6 Unsolicited PII 16
4.4.7 Sensitive PII 16
4.5 Privacy safeguarding requirements 17
4.5.1 Legal and regulatory factors 18
4.5.2 Contractual factors 18
4.5.3 Business factors 19
4.5.4 Other factors 19
4.6 Privacy policies 20
4.7 Privacy controls 20

5 The privacy principles of ISO/IEC 29100 21
5.1 Overview of privacy principles 21
5.2 Consent and choice 21
5.3 Purpose legitimacy and specification 22
5.4 Collection limitation 22
5.5 Data minimization 23
5.6 Use, retention and disclosure limitation 23
5.7 Accuracy and quality 23
5.8 Openness, transparency and notice 24
5.9 Individual participation and access 24
5.10 Accountability 25
5.11 Information security 25
5.12 Privacy compliance 26

Annex A (informative) Correspondence between ISO/IEC 29100 concepts and ISO/IEC 27000 concepts 27

Bibliography 28

Figures

Figure 1 – Factors influencing privacy risk management 18

Tables

Table 1 – Possible flows of PII among the PII principal, PII controller, PII processor and a third party and their roles 14

Table 2 – Example of attributes that can be used to identify natural persons 15

Table 3 – The privacy principles of ISO/IEC 29100 21

Table A.1 – Matching ISO/IEC 29100 concepts to ISO/IEC 27000 concepts 27