ISO/IEC 29134:2023-05 (E)

Information technology - Security techniques - Guidelines for privacy impact assessment

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Abbreviated terms 3

5 Preparing the grounds for PIA 4
5.1 Benefits of carrying out a PIA 4
5.2 Objectives of PIA reporting 5
5.3 Accountability to conduct a PIA 5
5.4 Scale of a PIA 6

6 Guidance on the process for conducting a PIA 6
6.1 General 6
6.2 Determine whether a PIA is necessary (threshold analysis) 7
6.3 Preparation of the PIA 7
6.3.1 Set up the PIA team and provide it with direction 7
6.3.2 Prepare a PIA plan and determine the necessary resources for conducting the PIA 9
6.3.3 Describe what is being assessed 10
6.3.4 Stakeholder engagement 11
6.4 Perform the PIA 13
6.4.1 Identify information flows of PII 13
6.4.2 Analyse the implications of the use case 14
6.4.3 Determine the relevant privacy safeguarding requirements 15
6.4.4 Assess privacy risk 16
6.4.5 Prepare for treating privacy risks 19
6.5 Follow up the PIA 23
6.5.1 Prepare the report 23
6.5.2 Publication 24
6.5.3 Implement privacy risk treatment plans 24
6.5.4 Review and/or audit of the PIA 25
6.5.5 Reflect changes to the process 26

7 PIA report 26
7.1 General 26
7.2 Report structure 27
7.3 Scope of PIA 27
7.3.1 Process under evaluation 27
7.3.2 Risk criteria 29
7.3.3 Resources and people involved 29
7.3.4 Stakeholder consultation 29
7.4 Privacy requirements 29
7.5 Risk assessment 29
7.5.1 Risk sources 29
7.5.2 Threats and their likelihood 29

7.5.3 Consequences and their level of impact 30
7.5.4 Risk evaluation 30
7.5.5 Compliance analysis 30
7.6 Risk treatment plan 30
7.7 Conclusion and decisions 30
7.8 PIA public summary 30

Annex A (informative) Scale criteria on the level of impact and on the likelihood 32

ISO/IEC 29134:2023(E) Annex B (informative) Generic threats 34

Annex C (informative) Guidance on the understanding of terms used 38

Annex D (informative) Illustrated examples supporting the PIA process 41

Bibliography 43