DIN EN ISO/IEC 29134:2020-09 (E)

Information technology - Security techniques - Guidelines for privacy impact assessmen t (ISO/IEC 29134:2017)

Contents

Page

European foreword ... **4**

Foreword ... **5**

Introduction ... **6**

1 Scope ... **7**

2 Normative references ... **7**

3 Terms and definitions ... **7**

4 Abbreviated terms ... **9**

5 Preparing the grounds for PIA ... **10**
5.1 Benefits of carrying out a PIA ... 10
5.2 Objectives of PIA reporting ... 11
5.3 Accountability to conduct a PIA ... 11
5.4 Scale of a PIA ... 12

6 Guidance on the process for conducting a PIA ... **12**
6.1 General ... 12
6.2 Determine whether a PIA is necessary (threshold analysis) ... 13
6.3 Preparation of the PIA ... 13
6.3.1 Set up the PIA team and provide it with direction ... 13
6.3.2 Prepare a PIA plan and determine the necessary resources for conducting the PIA ... 15
6.3.3 Describe what is being assessed ... 16
6.3.4 Stakeholder engagement ... 17
6.4 Perform the PIA ... 19
6.4.1 Identify information flows of PII ... 19
6.4.2 Analyse the implications of the use case ... 20
6.4.3 Determine the relevant privacy safeguarding requirements ... 21
6.4.4 Assess privacy risk ... 22
6.4.5 Prepare for treating privacy risks ... 25
6.5 Follow up the PIA ... 29
6.5.1 Prepare the report ... 29
6.5.2 Publication ... 30
6.5.3 Implement privacy risk treatment plans ... 30
6.5.4 Review and/or audit of the PIA ... 31
6.5.5 Reflect changes to the process ... 32

7 PIA report ... **32**
7.1 General ... 32
7.2 Report structure ... 33
7.3 Scope of PIA ... 33
7.3.1 Process under evaluation ... 33
7.3.2 Risk criteria ... 35
7.3.3 Resources and people involved ... 35
7.3.4 Stakeholder consultation ... 35
7.4 Privacy requirements ... 35
7.5 Risk assessment ... 35
7.5.1 Risk sources ... 35
7.5.2 Threats and their likelihood ... 35
7.5.3 Consequences and their level of impact ... 36
7.5.4 Risk evaluation ... 36

7.5.5 Compliance analysis 36
7.6 Risk treatment plan 36
7.7 Conclusion and decisions 36
7.8 PIA public summary 36

Annex A (informative) **Scale criteria on the level of impact and on the likelihood** **38**
Annex B (informative) **Generic threats** **40**
Annex C (informative) **Guidance on the understanding of terms used** **44**
Annex D (informative) **Illustrated examples supporting the PIA process** **46**
Bibliography **48**