DIN EN 17799:2024-09 (E)

Personal data protection requirements for processing operations

Contents

Page

European foreword 4

Introduction 5

1 Scope 6

2 Normative references 6

3 Terms and definitions 6

4 Overview 7

5 Planning 7
5.1 General 7
5.2 Understanding the needs and expectations of interested parties 7
5.3 Scope of personal data processing activities 7
5.3.1 General 7
5.3.2 Records of data processing activities 8
5.3.3 Identification of the legal basis 8
5.3.4 Data minimization 9
5.3.5 Retention periods 9
5.4 Policy for personal data protection 9
5.5 Roles and responsibilities 10
5.5.1 General 10
5.5.2 Internal roles 11
5.5.3 External roles 11
5.6 Risk management 12
5.6.1 General 12
5.6.2 Data protection risk assessment and impact analysis 12
5.6.3 Evaluation of the impact on data protection 13
5.6.4 Risk treatment and treatment plan 14
5.7 Personal data protection by design and by default 14

6 Operational activities 15
6.1 General 15
6.2 Data protection notices and consent 15
6.2.1 Data protection notices 15
6.2.2 Consent 15
6.3 Update of roles 16
6.4 Personal data protection 16
6.4.1 Erasure of data 16
6.4.2 Implementation and maintenance of security measures 16
6.4.3 Management of personal data breaches 17
6.5 Data subjects' requests for the application of their rights 18
6.5.1 General 18
6.5.2 Data access 18
6.5.3 Correction 18
6.5.4 Erasure 19
6.5.5 Restriction of processing 19
6.5.6 Data portability 19
6.5.7 Objections 19
6.5.8 Automated decisions, including profiling 20

6.5.9 Complaints and appeals 20
6.6 Training and awareness 20

7 Control 20
7.1 General 20
7.2 Internal audits 20
7.3 Periodical report 21
7.4 Nonconformities and corrective actions 22

Annex A (informative) Controllers and processors requirements mapping 23

Bibliography 25