ISO/IEC 27559:2022-11 (E)

Information security, cybersecurity and privacy protection - Privacy enhancing data de-identification framework

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 3

5 Overview 3

6 Context assessment 4
6.1 General 4
6.2 Threat modelling 4
6.2.1 General 4
6.2.2 Security and privacy practices 5
6.2.3 Motives and capacity to re-identify 5
6.3 Transparency and impact assessment 6
6.3.1 General 6
6.3.2 Transparency of actions and stakeholder engagement 6
6.3.3 Privacy-related harms 6

7 Data assessment 7
7.1 General 7
7.2 Data features 7
7.2.1 General 7
7.2.2 Data principals 7
7.2.3 Data type 7
7.2.4 Attribute types 8
7.2.5 Dataset properties 8
7.3 Attack modelling 8
7.3.1 General 8
7.3.2 Maximum or average risk 9
7.3.3 Population or sample-based attack 9
7.3.4 Data privacy models 9

8 Identifiability assessment and mitigation 10
8.1 General 10
8.2 Assessing identifiability 10
8.2.1 General 10
8.2.2 Quantifying identifiability 10
8.2.3 Adversarial testing 11
8.3 Mitigation 12
8.3.1 General 12
8.3.2 Reconfiguring the environment 12
8.3.3 Transforming the data 12
8.3.4 Re-evaluation 13

9 De-identification governance 13
9.1 General 13
9.2 Before data are made available 13
9.2.1 General 13
9.2.2 Assigning roles and responsibilities 13
9.2.3 Establishing principles, policies and procedures 14
9.2.4 Identifying and managing a data disclosure 14
9.2.5 Communicating with stakeholders 15
9.3 After data are made available 15
9.3.1 General 15
9.3.2 Monitoring the data environment 15
9.4 Mitigation in case of incident 15

Annex A (informative) Example identifiers 17

Annex B (informative) Example threshold identifiability benchmarks 19

Bibliography 21