

# ISO/IEC 27561:2024-03 (E)

## Information security, cybersecurity and privacy protection - Privacy operationalisation model and method for engineering (POMME)

---

### Contents

Page

Foreword..... iv

Introduction..... v

**1 Scope..... 1**

**2 Normative references..... 1**

**3 Terms and definitions..... 1**

**4 Symbols and abbreviated terms..... 7**

**5 Context of privacy operationalization..... 7**

5.1 General..... 7

5.2 Privacy engineering viewpoint..... 7

5.3 Privacy engineering operationalization model..... 8

5.4 Privacy engineering operationalization method..... 8

5.5 POMME processes overview..... 8

5.6 Privacy and security..... 9

**6 Initial information inventory process..... 10**

6.1 Purpose..... 10

6.2 Outcomes..... 10

6.3 Define and describe the TOA..... 10

6.4 Participant and information source identification..... 11

6.5 Systems and processes identification..... 11

6.6 Domains and domain owners identification..... 11

6.7 Intra-domain roles and responsibilities identification..... 12

6.8 Touch points identification..... 12

6.9 Data flows identification..... 12

6.10 PII identification..... 12

**7 Privacy controls, privacy control requirements, capabilities, risk assessment and iteration process..... 13**

7.1 Purpose..... 13

7.2 Outcomes..... 13

7.3 Privacy control specification..... 14

7.4 Privacy control requirement specification..... 14

7.5 Capabilities specification..... 14

7.6 Risk assessment..... 15

7.7 Iteration..... 15

**8 Privacy capabilities..... 16**

8.1 Capabilities overview..... 16

8.2 Capability details and associated functions..... 17

8.2.1 Core policy capabilities..... 17

8.2.2 Privacy assurance capabilities..... 18

8.2.3 Presentation and lifecycle capabilities..... 18

**Annex A (informative) Mapping of the privacy principles from ISO/IEC 29100 to POMME capabilities..... 19**

**Annex B (informative) Lifecycle process example involving a PII controller and a solution provider..... 20**

**Annex C (informative) POMME capability functions and mechanisms in a consumer application use case..... 23**

**Bibliography..... 28**