DIN EN 14484:2004-03 (E)

Health informatics_- International transfer of personal health data covered by the EU data protection directive_- High level security policy; German version EN_14484:2003, text in English

Contents

Page

Foreword ... 5

Introduction ... 6

1 Scope ... 10

2 Normative references ... 10

3 Terms and definitions ... 10

4 Abbreviated terms ... 11

5 The European Data Protection Directive (see annex A) ... 12
5.1 General ... 12
5.2 General aims: (Article 1) ... 12
5.3 Scope: electronic and non-electronic (Article 3) ... 12
5.4 Principles relating to data quality (Article 6) ... 12
5.5 Criteria for legitimacy (Article 7) ... 12
5.6 Special categories of processing, including personal health data (Article 8) ... 13
5.7 Information to be given to the data subject (Article 10) ... 13
5.8 Right of access to data (Article 12) ... 13
5.9 Right to object (Article 14) ... 13
5.10 Security of processing (Article 17) ... 14
5.11 Judicial remedies, liability and sanctions (Articles 22, 23 and 24) ... 14
5.12 Supervisory Authorities (Articles 28 and 18) ... 14
5.13 Working party on the protection of Individuals with regard to the Processing of Personal Data ... 14
5.14 Transfer of personal data to Third Countries ... 14

6 Requirements for the transfer of personal data to third Countries. ... 14
6.1 General ... 14
6.2 Principles (Article 25) ... 14
6.3 Ensuring transfers are permissible ... 15
6.4 Grounds by which transfers to third countries are permissible ... 15
6.4.1 General ... 15
6.4.2 Members of the EEA ... 15
6.4.3 Depersonalisation of data ... 15
6.4.4 Consent ... 16
6.4.5 Subject to contract clauses ... 16
6.4.6 Claiming adequacy of data protection ... 17

7 A Security Policy for third countries ... 17
7.1 The requirement ... 17
7.2 The purpose of the security policy ... 18
7.3 The 'level' of the security policy ... 18

8 High Level Security Policy: general aspects ... 18
8.1 Levels of abstraction in ensuring security ... 18
8.2 Generic principles ... 18
8.3 Non-generic Principles ... 19
8.4 Guidelines ... 19
8.5 Measures ... 19
8.6 Elements of a High Level Security Policy ... 19

9 High Level Security Policy: the content ... 19
9.1 Principle One: overriding generic principle ... 19
9.1.1 General ... 19
9.1.2 Principle One, Guideline One: fundamental rights and freedoms ... 19
9.1.3 Principle One, Guideline Two: information about doubts ... 20

Page

9.1.4 Rationale ... 20
9.1.5 Observations as to Measures ... 20
9.2 Principle Two: chief executive support ... 20
9.2.1 General ... 20
9.2.2 Principle Two, Guideline One: alignment with local practice ... 20
9.2.3 Principle Two, Guideline Two: organisational arrangements ... 20
9.2.4 Principle Two, Guideline Three: regular HLSP review ... 20
9.2.5 Rationale ... 20
9.2.6 Observations as to Measures ... 20
9.3 Principle Three: documentation of Measures and review ... 21
9.3.1 General ... 21
9.3.2 Principle Three, Guideline One: staff information ... 21
9.3.3 Rationale ... 21
9.3.4 Observations as to Measures ... 21
9.4 Principle Four: Data Protection Security Officer ... 21
9.4.1 General ... 21
9.4.2 Principle Four, Guideline One: Data Protection Security Officer and organisation as a processor ... 21
9.4.3 Principle Four, Guideline Two: Data Protection Security Officer and organisation as a controller ... 21
9.4.4 Principle Four, Guideline Three: Data Protection Security Officer qualification for office ... 21
9.4.5 Rationale ... 21
9.4.6 Observations on Measures ... 22
9.5 Principle Five: permission to process ... 22
9.5.1 General ... 22
9.5.2 Principle Five, Guideline One: unambiguous consent to transfer ... 22
9.5.3 Principle Five, Guideline Two: explicit consent to processing ... 22
9.5.4 Principle Five, Guideline Three: limitation to the purposes consented ... 22
9.5.5 Principle Five, Guideline Four: conditional consents ... 22
9.5.6 Principle Five, Guideline Five: review of information concerning consent ... 22
9.5.7 Rationale ... 22
9.5.8 Observations regarding Measures ... 23
9.6 Principle Six: information about processing ... 23
9.6.1 General ... 23
9.6.2 Principle Six, Guideline One: documentation about consented processing ... 23
9.6.3 Principle Six, Guideline Two: quality of data collected and processed ... 23
9.6.4 Principle Six, Guideline Three: accuracy of data processed ... 23
9.6.5 Principle Six, Guideline Four: Data Retention and Destruction Policy ... 23
9.6.6 Principle Six, Guideline Five: data subjects' access to their data ... 23
9.6.7 Principle Six, Guideline Six: objection to processing ... 23
9.6.8 Principle Six, Guideline Seven: rectification, erasure and blocking ... 23
9.6.9 Principle Six, Guideline Eight: identification of transferred data ... 24
9.6.10 Principle Six, Guideline Nine: action on notification of the death of a data subject ... 24
9.6.11 Principle Six, Guideline Ten: direct marketing ... 24
9.6.12 Principle Six, Guideline Eleven: re-personalisation of de-personalised data ... 24
9.6.13 Observations on Measures ... 24
9.7 Principle Seven: information for the data subject ... 25
9.7.1 General ... 25
9.7.2 Rationale ... 25
9.7.3 Observations on Measures ... 25
9.8 Principle Eight: prohibition of onward data transfer without consent ... 25
9.8.1 General ... 25
9.8.2 Principle Eight, Guideline One: assuring protection for onward transfers ... 25
9.8.3 Principle Eight, Guideline Two: HLSP for onward transfers ... 25
9.8.4 Principle Eight, Guideline Three: Disclosure Register ... 25
9.8.5 Rationale ... 25
9.9 Principle Nine: remedies and compensation ... 26
9.9.1 General ... 26

Page

9.9.2 Principle Nine, Guideline One: investigation of complaints ... **26**
9.9.3 Principle Nine, Guideline Two: independent arbitration ... **26**
9.9.4 Rationale ... **26**
9.9.5 Observations on Measures ... **26**
9.10 Principle Ten: security of processing ... **26**
9.10.1 General ... **26**
9.10.2 Principle Ten, Guideline One: risk analysis ... **26**
9.10.3 Principle Ten, Guideline Two: encryption during transmission ... **27**
9.10.4 Principle Ten, Guideline Three: proof of data integrity and authentication of origin ... **27**
9.10.5 Principle Ten, Guideline Four: access control and user authentication ... **27**
9.10.6 Principle Ten, Guideline Five: Physical and Environmental Security ... **27**
9.10.7 Principle Ten, Guideline Six: application management ... **27**
9.10.8 Principle Ten, Guideline Seven: network management ... **27**
9.10.9 Principle Ten, Guideline Eight: virus controls ... **27**
9.10.10 Principle Ten, Guideline Nine: reporting breaches of security ... **27**
9.10.11 Principle Ten, Guideline Ten: Business Continuity Plans ... **27**
9.10.12 Principle Ten, Guideline Eleven; audit trails ... **27**
9.10.13 Principle Ten, Guideline Twelve: handling particularly sensitive data ... **27**
9.10.14 Rationale and observations on Measures ... **27**
9.11 Principle Eleven: responsibilities of staff and other contractors ... **28**
9.11.1 General ... **28**
9.11.2 Principle Eleven, Guideline One: informing staff and other contractors ... **28**
9.11.3 Principle Eleven, Guideline Two: instruction and training ... **28**
9.11.4 Principle Eleven, Guideline Three: staff and contractor contractual obligations ... **28**
9.11.5 Rationale ... **28**
9.11.6 Observation on Measures ... **28**
9.12 Principle Twelve: adequacy of third country data protection ... **28**
9.12.1 General ... **28**
9.12.2 Rationale ... **28**
9.12.3 Observations on Measures ... **28**
9.13 Principle Thirteen: additional EU Member State particular requirements ... **28**
9.13.1 Rationale ... **29**
9.13.2 Observations on Measures ... **29**
10 Rationale and Observations on Measures to support Principle Ten concerning security of processing ... **29**
10.1 General ... **29**
10.2 Encryption and digital signatures for transmission to the third country ... **29**
10.3 Access controls and user authentication ... **29**
10.4 Audit Trails ... **30**
10.5 Physical and environmental security ... **30**
10.6 Application management and network management ... **30**
10.7 Viruses ... **30**
10.8 Breaches of security ... **30**
10.9 Business Continuity Plan ... **30**
10.10 Handling particularly sensitive data ... **30**
10.11 Standards ... **31**
11 Personal health data in non-electronic form ... **31**
Annex A (normative) **EU Data Protection Directive** ... **32**
Annex B (informative) **Useful sources of advice** ... **53**
B.1 EU Security projects ... **53**
B.2 CEN/ISSS ... **53**
B.3 Non-CEN Standards ... **53**
B.4 Selected web sites ... **54**
Annex C (informative) **Model declaration** ... **55**
Bibliography ... **57**