



PRC/RIA

Appendix 2 Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

1 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

This Appendix is made by and between the Information System Authority of the Republic of Estonia and the Population Centre of Finland and is an integral part of the General Agreement (PRC 2286/2401/16; RIA 16-0448-001) concerning the Trust Federation of Estonian X-Tee and Finnish Palveluväylä.

Trust Federation of Estonia X-tee and Finnish Palveluväylä

APPENDIX 2 - RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

Table of contents

1. Relevant national regulation in Finland in relations of execution of Trust Federation and to inform the members of X-tee or Palveluväylä	2
1.1. General Regulation	2
1.2. Special Regulation	6
2. Relevant national regulation in Estonia in relations of execution of Trust Federation and to inform the members of X-tee or Palveluväylä	7
2.1. General regulation	7
2.2. Special Regulation	9
3. EU Regulation.....	10



PRC/RIA

Appendix 2
Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

2 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

1. Relevant national regulation in Finland in relations of execution of Trust Federation and to inform the members of X-tee or Palveluväylä

1.1. General Regulation

Finnish	English	Comments
Asetus tietoturvallisuudesta valtionhallinnossa (681/2010)	Government Decree on information security in central government (681/2010)	<ul style="list-style-type: none">- Sections 1- 23 Decree contains provisions on the general information security requirements applicable to the handling of documents by central government authorities, on the grounds for classifying documents, and on the information security requirements corresponding to the classification and applicable to the handling of documents.
Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)	Decree on the Openness of Government Activities and on Good Practice in Information Management (1030/1999)	<ul style="list-style-type: none">- Section 1 Assessments in support of good practice in information management- Section 4 Instructions, supervision and monitoring- Section 8 Information system descriptions
Hallintolaki (434/2003)	Administrative Procedure Act (434/2003)	<ul style="list-style-type: none">- It is the objective of this Act to achieve and promote good administration and access to justice in administrative matters. It is further the objective of this Act to promote the quality and productivity of administrative services.- Section 6 Legal principles of administration- Section 24 Openness of consideration- Sections 54 - 63 Service of administrative decisions and other documents
Henkilötietolaki (523/1999)	Personal Data Act (523/1999)	<ul style="list-style-type: none">- Section 5 Duty of care- Section 6 Defined purpose of processing data- Section 7 Exclusivity of purpose- Section 8 General prerequisites for processing- Section 9 Principles relating to data quality- Section 10 Description of file- Section 11 Prohibition to process sensitive data- Chapter 9 Section 48 Penal provisions
Laki Hallinnon yhteisistä sähköisen asiainnin tukipalveluista (571/2016)	Act on common administrative e-service support services (571/2016)	<ul style="list-style-type: none">-



PRC/RIA

Appendix 2
Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

3 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

Finnish	English	Comments
Laki huoltovarmuuden turvaamisesta (225/2008)	Act on Safeguarding Security of Supply (225/2008)	<ul style="list-style-type: none">- Section 1 Objective of the Act- Section 2 Sufficient readiness under all circumstances- Section 16 Provision authorising the Government to issue more detailed provisions by Decree
Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015)	Act on Government Security Network activities (10/2015)	<ul style="list-style-type: none">-
Laki kansainvälisistä tietoturvaselvityksistä (588/2001)	Act on International Information Security Obligations (588/2001)	<ul style="list-style-type: none">- Section 6 Secrecy and use of information- Section 7 Professional secrecy and the prohibition of exploitation- Section 8 Security classification markings- Section 9 Protection levels indicating handling requirements- Section 10 Security requirements concerning premises- Section 11 Personnel security clearances and reviews- Section 12 Facility security clearances and reviews- Section 19 Investigating and notifying of violations
Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)	Act on Electronic Services and Communication in the Public Sector (13/2003)	<ul style="list-style-type: none">- Section 1 Objective of the Act- Section 5 Availability of electronic services- Section 6 Accessibility of the authorities Section 13 Recording and registration of electronic documents- Section 21 Archiving
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (533/2016)	Act on Strong Electronic Identification and Electronic Trust Services (533/2016)	
Laki Valtion yhteisten tieto- ja viestintätekniisten palvelujen järjestämisestä (1226/2013)	Act on the Organisation of Shared Information and Communications Technology Services in Central Government (1226/2013)	



PRC/RIA

Appendix 2
Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

4 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

Finnish	English	Comments
Laki viranomaisen toiminnan julkisuudesta (621/1999)	Act on the Openness of Government Activities (621/1999)	<ul style="list-style-type: none">- Section 1 Principle of openness- Section 3 Duty to promote good practice on information management- Section 10 Access to a secret document- Chapter 5: Duty of the authorities to promote access and good practice on information management- Chapter 6 Secrecy obligations- Chapter 7 Derogations from secrecy and declassification
Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)	Act on the Evaluation of Government Information Systems and Data Transfer Arrangements (Act 1406/2011)	<ul style="list-style-type: none">- Section 3 Using evaluation agencies on information security- Section 6 The Finnish Communications Regulatory Authority's right to information and right to enter the premises and information systems
Rikoslaki (39/1889)	The Criminal Code of Finland (39/1889)	<ul style="list-style-type: none">- Chapter 28 Section 7 Unauthorised use (769/1990)- Chapter 28 Section 8 Aggravated unauthorised use- Chapter 28 Section 9 Petty unauthorised use- Chapter 34 Section 1 Criminal mischief (578/1995)- Chapter 34 Section 9 a Endangerment of data processing (951/1999)- Chapter 35 Section 1 Criminal damage (769/1990)- Chapter 35 Section 2 Aggravated criminal damage- Chapter 35 Section 3 Petty criminal damage- Chapter 38 Section 1 Secrecy offence (578/1995)- Chapter 38 Section 2 Secrecy violation- Chapter 38 Section 3 Message interception (531/2000)- Chapter 38 Section 4 Aggravated message interception (578/1995)- Chapter 38 Section 5 Interference with communications (578/1995)- Chapter 38 Section 6 Aggravated interference with communications- Chapter 38 Section 7 Petty interference with communications- Chapter 38 Section 8 Computer break-in (578/1995)- Chapter 38 Section 8a Offence involving an illicit device for accessing protected services (1118/2001)- Chapter 38 Section 9 (1) Data protection offence (525/1999)- Chapter 40 Section 5 Breach and negligent breach of official secrecy (604/2002)



PRC/RIA

Appendix 2
Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

5 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

Finnish	English	Comments
Suomen perustuslaki (731/1999)	The Constitution of Finland (731/1999)	<ul style="list-style-type: none">- Section 7 The right to life, personal liberty and integrity- Section 10 The right to privacy- Section 12 Freedom of expression and right of access to information- Section 22 Protection of basic rights and liberties- Section 107 Subordination of lower-level statutes
Tietoyhteiskuntakaari (917/2014)	Information Society Code (917/2014)	<ul style="list-style-type: none">- Chapter 17 Processing Electronic Messages and Traffic Data- Chapter 18 Special Provisions for Corporate or Association Subscribers- Chapter 19 Information Related to Authorities- Chapter 33 (Sections 272-276) Management of Information Security and Interference and Related Notifications- Section 72 Communications network construction and maintenance work and measures related to information security- Section 90 Obligation of a telecommunications operator to prepare for exceptional circumstances- Section 128 Quality requirements for communications networks and communications services
Valmiuslaki (1080/1991)	Emergency Powers Act (1080/1991)	<ul style="list-style-type: none">- Chapter 6 Preparedness
Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä VAHTI 7/2009 26.11.2009	The Government Resolution on Enhancing Information Security in Central Government VAHTI 7/2009 26.11.2009	<ul style="list-style-type: none">- The Resolution sets out guidelines for central government to enhance information security as a key aspect of leadership and management, competence, risk management, and administrative reforms and activities.



PRC/RIA

Appendix 2
Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

6 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

1.2. Special Regulation

Asetus väestötietojärjestelmästä (128/2010)	Decree on the Population Information System. (128/2010)	
Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009)	Act on the Population Information System and the Certificate Services of the Population Register Centre (661/2009)	<ul style="list-style-type: none">- Section 1 Purpose of the Act- Section 26 Disclosure of information- Chapter 4 Public access to and disclosure of information from the Population Information System- Section 37 Processing of data subject to security prohibition- Section 44 Report on the use and protection of data- Section 45 When the restrictions on disclosure of information ceases- Section 46 Ways and means to provide information- Section 52 Population right to receive information and conduct inspections- Section 53 User Index- Section 56 Log Records- Section 59 Processing of event data- Section 60 Population Information System's Obligation to report- Section 67 Application for and issue of other certificates- Section 73 Data Systems Availability- Section 74 Data protection



PRC/RIA

Appendix 2
Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

7 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

2. Relevant national regulation in Estonia in relations of execution of Trust Federation and to inform the members of X-tee or Palveluväylä

2.1. General regulation

Regulation	Comments
Public Information Act¹ (avaliku teabe seadus ¹) § 43 ⁹ section 5	The obligation to exchange data through the X-Road with the databases belonging to the state information system and between the databases belonging to the state information system. This simply means that the X-Road is a mandatory data exchange layer for public sector.
Public Information Act¹ (avaliku teabe seadus ¹) § 43 ⁹ section 6	Although the X-Road is a mandatory data exchange layer for exchanging data with the databases belonging to the state information system and between the databases belonging to the state information system, other legal persons may use the X-Road for data exchange as well. The X-Road is a voluntary for private sector users, they are free to apply membership to X-Road. Both public and private sector members must follow the requirements provided in the X-Road regulation and in the affiliation agreement.
Public Information Act¹ (avaliku teabe seadus ¹) § 35	Grounds for classification of information as internal (restricted information to which access is restricted). Members (if they are holders of information (§ 5)) must be aware that during the data exchange they do not disclose any information which contains entirely or partially restricted information. The obligations of holders of information extend to state and local government agencies, legal persons in public law, legal persons in private law and natural persons if the persons perform public duties pursuant to law, administrative legislation or contracts, including the provision of educational, health care, social or other public services, – with regard to information concerning the performance of their duties. Deemed to be equal to holders of information are undertakings which have a dominant position in the market or special or exclusive rights or which are natural monopolies – with regard to information concerning the conditions and prices of the supply of goods and services and changes thereto; sole proprietors, non-profit associations, foundations and companies – with regard to information concerning the use of funds allocated from the state or a local government budget for the performance of public duties or as support. Estonian Public Information Act is compatible with Directive 2003/98/EC of the European Parliament and of the Council on the re-use of public sector information and Directive 2013/37/EU of the European Parliament and of the Council amending Directive 2003/98/EC on the re-use of public sector information. Competent authority - Estonian Data Protection Inspectorate, website: http://www.aki.ee/en .



PRC/RIA

Appendix 2
Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

8 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

Regulation	Comments
<p>Government of the Republic Regulation 23.09.2016 no 105 "The data exchange layer of information systems" (Vabariigi Valitsuse 23.09.2016 määrus nr 105 "Infosüsteemide andmevahetuskiht").</p> <p>Unofficial translation available: https://www.ria.ee/public/x_tee/The-data-exchange-layer-regulation.pdf.</p>	<p>The main requirements for operating, administering and exploiting X-Road. It also establishes members' general rights, obligations and responsibilities.</p> <p>More information: https://www.ria.ee/en/x-road.html</p>
<p>Government of the Republic Regulation 20.12.2007 no 252 "The system of security measures for information systems" (Vabariigi Valitsuse 20.12.2007 määrus nr 252 "Infosüsteemide turvameetmete süsteem")</p>	<p>Security requirements for public sector members' information systems are established in the three-level IT baseline security system ISKE. As well as the X-Road, the ISKE is also one of the support systems to state information system. The goal of implementing ISKE is to ensure a security level sufficient for the data processed in IT systems. The necessary security level is achieved by implementing the standard organizational, infrastructural/physical and technical security measures.</p> <p>ISKE is compulsory for state and local government organizations who handle databases.</p> <p>An X-Road member shall implement measures to ensure the integrity, confidentiality, and processability of the data in order to alleviate security risks and ensure independent auditing of the measures applied at least once in every four years. In managing a national or local government unit's database, an X-Road member shall be implementing the measures for ensuring integrity, confidentiality, and processability and in ensuring independent auditing of the applied measures in accordance with ISKE regulation.</p> <p>More information: https://www.ria.ee/en/iske-en.html</p>
<p>Government of the Republic Regulation 28.02.2008 no 58 "the administration system of the state information system" (Vabariigi Valitsuse 28.02.2008 määrus nr 58 "Riigi infosüsteemi haldussüsteem")</p>	<p>Members' databases themselves must be registered in the administration system for the state information system RIHA. RIHA serves as a catalogue for the state's information system. At the same time, it is a procedural and administrative environment via which the comprehensive and balanced development of the state's information system is ensured. RIHA guarantees the transparency of the administration of the state's information system and helps to plan the state's information management.</p> <p>Applications for affiliation of membership to X-Road shall be filed through RIHA.</p> <p>An X-Road member shall also keep the details submitted to RIHA updated and forward any X-Road related applications and the information specified in clause 6 of this subsection to the RIA through RIHA.</p> <p>RIA shall have the right to reject an affiliation application to X-Road if the applicant's details submitted upon affiliation are not registered in RIHA or the details are not up-to-date.</p>



PRC/RIA

Appendix 2
Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

9 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

Regulation	Comments
	<p>In order to register a subsystem on X-Road, the X-Road member shall submit an application to the RIA through RIHA and only these subsystems will be registered on X-Road that are entered into RIHA. Dataservice must be entered into RIHA as well and dataservice provider shall ensure that the description of the dataservice in RIHA is relevant and updated.</p> <p>More information: https://www.ria.ee/en/administration-system-of-the-state-information-system.html https://riha.eesti.ee/riha/main</p>
<u>Personal Data Protection Act¹</u> (isikuandmete kaitse seadus ²) § 10 section 2	<p>X-Road members must follow the Personal Data Protection Act while exchanging personal data. Processing (including exchange) of personal data is permitted only with the consent of the data subject unless otherwise provided by law. An administrative authority shall process (without the consent of the data subject) personal data only in the course of performance of public duties in order to perform obligations prescribed by law, an international agreement or directly applicable legislation of the Council of the European Union or the European Commission.</p> <p>Estonian Personal Data Protection act is compatible with Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.</p> <p>Estonian Data Protection Inspectorate website: http://www.aki.ee/en.</p>
<u>Electronic Identification and Trust Services for Electronic Transactions Act</u> (E-identimise ja e-tehingute usaldusteenuste seadus)	<p>This Act regulates electronic identification and trust services for electronic transactions, and organisation of state supervision to the extent that these are not regulated by Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.</p>

2.2. Special Regulation

RIA guidelines	<p>RIA has established several guidelines for members as well as to specify the requirements provided by law</p> <p>More information https://www.ria.ee/en/x-road-instructions.html</p>
----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



PRC/RIA

Appendix 2 Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

10 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

	Note: Please notice that Trust Federation is applicable if members have joined the X-Road v6. Therefore should be most relevant guidelines related to X-Road v6.
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. EU Regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR)	National authorities in the Member States should cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State. Note: GDPR shall apply from 25 May 2018. Directive 95/46/EC is repealed with effect from 25 May 2018.
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data	Note: Directive 95/46/EC is repealed with effect from 25 May 2018.
Treaty Of Lisbon (2007/C 306/01)	Basis for free data movement.
The article 29 Data Protection Working Party opinions and recommendations	The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	This regulation lays down rules for trust services, in particular for electronic transactions and establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	This regulation establishes security and notification requirements for operators of essential services and for digital service providers.



PRC/RIA

Appendix 2
Trust Federation

PRC 2286/2401/16
RIA 16-0448-001

11 (11)

28.6.2017

RELEVANT NATIONAL REGULATION FOR THE EXECUTION OF TRUST FEDERATION

4. This Appendix is an integral part of the General Agreement (PRC 2286/2401/16; RIA 16-0448-001) concerning the Trust Federation of Estonian X-Tee and Finnish Palveluväylä.

5. Parties must notify each other if any changes in articles 1-2 occur or if additional relevant regulation comes into force. Previously mentioned notification shall be in a written form.