Implementation of the MoReq2 Model Requirements for the Management of Electronic Records in Estonia

(Estonian “chapter zero” for MoReq2)

Version 2.0

2012
The implementation of MoReq2 in Estonia
Table of contents

Implementation of the MoReq2 Model Requirements for the Management of Electronic Records in Estonia................................................................. 1

1. INTRODUCTION........................................................................................................ 5
  2.1 Preparing and validating the translation................................................................ 6
  2.2 Language of the translation.................................................................................. 6
  2.3 Faithfulness of the translation to the original text.................................................. 6
  2.4 Translation of terminology.................................................................................. 7
  2.5 Estonian chapter zero........................................................................................... 14
  2.6 Publication of the translation of MoReq2 and chapter zero..................................... 15

3 ESTONIAN NATIONAL CHARACTERISTICS: DEVELOPMENT OF RECORDS MANAGEMENT AND THE REGULATORY ENVIRONMENT.............................................. 16
  3.1 The organisation of records management in Estonia............................................. 16
  3.2 Legislation, standards and guideline that apply to the field..................................... 17

4 ESTONIAN NATIONAL CHARACTERISTICS: ERMSs AS A PART OF THE STATE INFORMATION SYSTEM............................................................................................. 21
  4.1 Development of information society, the interoperability framework and paperless administration............................................................................ 21
  4.2 State information system ..................................................................................... 21
  4.3 Administration system of state information system (RIHA) and its components...... 23
  4.4 Information systems’ data exchange layer X-Road and the State Portal............... 24
  4.5 Document Exchange Centre (DEC)...................................................................... 25

5 ESTONIAN NATIONAL CHARACTERISTICS: E-IDENTITY AND INFORMATION SECURITY.................................................................................................................. 29
  5.1 Estonian personal identification code and digital identity documents....................... 29
  5.2 Estonian digital signatures and stamps: authentication and encryption.................. 30
  5.3 ISKE: a three-level baseline security system for information systems.................... 34

6 ESTONIAN NATIONAL CHARACTERISTICS: NATIONAL REQUIREMENTS FOR ERMSs .................................................................................................................. 36
  6.1 Main requirements for ERMSs as outlined in legislation....................................... 36
  6.2 Classification scheme and list of record classes..................................................... 36
  6.3 Metadata for records and aggregations of records................................................ 37
  6.4 Creation and exchange of records......................................................................... 38
6.5 Registration and disclosure of records ................................................................. 41
6.6 Retention, disposition, transfer to the National Archives and destruction of records .... 44
APPENDIX 1: DIFFERENCES BETWEEN THE TEXTS OF MoReq2 (v1.04) IN ENGLISH AND ESTONIAN ................................................................. 48
APPENDIX 2: FOOTNOTES IN THE ESTONIAN TRANSLATION OF MoReq2 ............... 54
APPENDIX 3: AMENDMENTS TO THE CHAPTER ZERO, 2012 (Version 2.0) .............. 59
Chapter “0” – MoReq Governance Board Approval .................................................. 61
1. INTRODUCTION

The original Moreq – Model Requirements for the Management of Electronic Records – was prepared for the European Commission in 2001 and was not translated into Estonian. In 2002, Riigikantselei (Government Office of the Republic of Estonia, hereinafter referred to as “the Government Office”)¹ prepared the national Requirements for the Functionality of Electronic Records Management Systems, which were primarily based on the MoReq model requirements, the ISO 15489 records management standard and the legislation governing records management in Estonia. The aforementioned requirements included aspects that are specific to the Estonian tradition of records management and legal regulations, such as: using the Estonian ID card for authentication, providing records with digital signatures, allowing public access to records' metadata through a web page, etc. Although the requirements were supplemented with an application guidance document and published online, following the requirements was not obligatory for public sector institutions. However, many electronic records management systems (ERMSs) have been procured or implemented based on the aforementioned requirements.

A new version of the Model Requirements, MoReq2, was prepared for the European Commission and published in 2008. By then, the Estonian national requirements had become obsolete. In order to harmonise Estonian requirements with the European ones, the Government Office decided not to update the national requirements, but to publish the translation of MoReq2, along with a description of Estonian national characteristics. Estonian national requirements are described in these guidelines, hereinafter called "chapter zero" as it follows the recommendation provided in MoReq2 section 1.9 for preparing “national chapters”: it describes terminology selections pertaining to the translation, requirements arising from national legislation and regulations, and other national exceptions, as well as contains references for further information. The chapter zero is published on the DLM Forum² website together with the translation of MoReq2, but as a separate document, which facilitates further reviews of the chapter zero.

On 1 January 2012, the function of coordinating the development of records management was transferred from the Government Office to the Ministry of Economic Affairs and Communications. In 2012, the ministry reviewed the chapter zero and made the necessary amendments and additions to reflect the developments which had taken place after publishing the first version.

¹ At the time, the Government Office coordinated the development of records management in the public sector of Estonia.
² DLM Forum is a body of international cooperation, which joins various parties involved in the information/records management and archiving in Europe and beyond. The DLM Forum was first summoned by the European Commission as far back as in 1996.
2. TRANSLATION AND PUBLICATION OF MOREQ2

2.1 Preparing and validating the translation

The Estonian translation is based on version 1.04 of MoReq2 which was completed in 2008; Appendix 9 will not be translated into Estonian. The translation project was carried out by the Records Management Department of the Government Office; the completed translation has been validated by the DLM-Forum.

Contributions were made to the translation process by Luisa Translation Bureau (initial draft) and Wiedemann Translation Company (linguistic equivalence assessment). Among the experts involved in discussions on terminology were lecturers on the speciality of records management from Tallinn University and the University of Tartu Viljandi Culture Academy as well as specialists from the National Archives of Estonia and the Estonian Informatics Centre (as of 1 June 2011 Estonian Information System’s Authority).

2.2 Language of the translation

MoReq2 is aimed at a wide range of users throughout the European Union and beyond. As a result, the document has been formulated so that it could be applied and put into practice for different purposes, including the testing of technological systems. Due to the comprehensive nature of the text, it is occasionally complicated and tends to consist of long sentences. In Estonia, where telegram-like briefness (i.e. a style in which sentences have been simplified as much as possible in the interest of clarity) is considered good style in official documents, the faithfulness of the translation to the original text unfortunately comes at some cost to good style. It has to be borne in mind, however, that MoReq2 is used for both developing and procuring ERMSs that comply with the MoReq2 specification. Thus, it is important that the requirements be interpreted identically in different languages, and therefore the main emphasis of the Estonian version is also on the accuracy of the translation and only thereafter on the fluency of expression. Explanations, figures and examples that have occasionally been supplemented with comments in footnotes by the translator have been provided in order to help the reader to understand MoReq2 better.

2.3 Faithfulness of the translation to the original text

As has been pointed out above, the translation of MoReq2 proceeded from the idea that the target text had to remain as faithful as possible to the source text. However, absolute equivalence or word-for-word translation cannot be achieved in the case of any target text, since languages differ from each other in terms of both vocabulary and grammar.

Comments on notable differences between the original text and the translation have been included in the Estonian version as footnotes. There are two types of differences: 1) those

---

3 The final draft of the MoReq2 translation and this section (Translation and Publication of MoReq2) of the chapter zero were prepared by Liivi Karlipštenko (the Government Office). The validation of the translation was carried out by Toivo Jullinen (National Archives) as the representative of the DLM Forum.
The implementation of MoReq2 in Estonia

caused by the distinct characteristics of the Estonian language and 2) those caused by mistakes in the original text. The latter have been collected in the table in Appendix 1 to this chapter zero and have been checked by the MoReq Governance Board (MGB) of the DLM Forum. In their e-mail of 28 February 2011, MGB confirmed that the changes in question were solely corrections of obvious mistakes and not changes of substance.

All footnotes added by the translator bear the marking “Tõlkija märkus” (translator’s comment). The footnotes provided in the original English language text and translated into Estonian have not been marked as translator’s comments.

It is important to bear in mind with regard to the differences that the English language original of MoReq2 and its Test Framework are used for ERMS testing and certification.

2.4 Translation of terminology

The key terms used in MoReq2 are defined in the MoReq2 glossary (section 13.1) and the key definitions are reproduced in section 2.1. Explanations regarding key terms and concepts are also provided in sections 2.2–2.3 and 13.2–13.3, as well as the introductions to some of the other sections.

The use of terminology in both the original English language version of MoReq2 and its Estonian translation is based on the attempt to use terms that correspond to common language usage or are widespread among experts in the field. This section explains and provides arguments for the use of those Estonian terms that are not in general use. The list also includes terms that have not been defined in the MoReq2 glossary but which proved to be problematic with regard to their translation into Estonian.

Record and document – dokument and teavik

As is the case with many other languages, the main difficulties in the Estonian environment have arisen from translating the terms record and document. Estonia is one of the cultures where a term similar to the English word document (in Estonian: dokument) has traditionally been used to refer to the concept denoted in English by the term record. The pronunciation and the spelling of the English word document are practically the same as that of the Estonian word, while the English term is also connected to the concept of documenting something. So far, the word dokument has been used in the Estonian translations of texts pertaining to records and archive management as the equivalent of both English terms (record and document).

However, a document is not the same as a record (see the definitions and explanations in the sections of MoReq2 referred to above). Due to this, the identical translation of two of the main terms related to records management has given rise to misunderstandings and questions in the past; in the case of the MoReq2 translation, the use of the same Estonian word for both terms would occasionally make the text completely incomprehensible. For example, the remark “However, note that some documents become records” in the definition of the term document would, in translation, be interpreted as “However, note that some

The implementation of MoReq2 in Estonia

documents become documents” or “However, note that some records become records” (in Estonian: Tuleb aga tähele panna, et mõnedest dokumentidest saavad dokumendid).

The records and archive management experts who participated in the discussions on MoReq2 terminology came to the conclusion that the definition of the term record as presented in the ISO 15489-1 standard as well as MoReq2 overlaps in essence with the Estonian definition of dokument as presented in Estonia’s Archives Act, according to which a dokument is “information recorded on any medium, which is created or received in the course of the activities of an agency or person, and the content, form and structure of which is sufficient to provide evidence of facts or activities.” Since this definition has been in use ever since the Archives Act was first published in 1998 and is widely recognised by Estonian experts in the field, it was determined that dokument should be used as the equivalent of record in Estonian and that a new translation should be found for the English term document.

Several translations were offered for the term document and eventually the Estonian term teavik was chosen as the most suitable equivalent. The choice of the aforementioned term was influenced by the following aspects:

- the term is short and easy to pronounce in Estonian;
- the term is related to the word teave (information);
- the term is also used as a translation equivalent of document in the field of information sciences and it is worth noting that the English definitions of the term document presented in MoReq2 and several information-related standards (e.g. ISO 5127 and ISO 2789) are virtually identical.

The experts considered it important to describe the way documents (teavikud) are related to information (teave) and records (dokumendid), which is visualised in the figure below: some information is recorded, forming documents; some documents are declared as records that have to be duly retained for as long as is necessary for use as a source of information or as evidence. Memory institutions permanently preserve records (but also documents), which have informational or evidential value that is not reduced even in a very long term and which are also expected to interest future historians.

---

5 Information sciences is an interdisciplinary field that also comprises records management, archival and librarian sciences. The term teavik has been adopted from the Estonian librarianship vocabulary where it has traditionally referred to material objects that contain information (e.g. books, magazines, discs, CDs, etc.); however, teavik can also refer to a set of data that is stored in a computer system and can be found, edited, etc. The terms teavikuhaldis and teavikuhaldussüsteem used in the Estonian translation of MoReq2 are not widely known.
It was decided in the course of the discussions, however, that the term teavik (as an equivalent for document) should initially be used in the Estonian translation of MoReq2 in order to ensure the ease of understanding of the contents and requirements of MoReq2; since the concept of teavik is not being commonly used in the field of records management, its suitability (or unsuitability) for general use will be revealed in time.

ERMS, EDMS, EDRMS – the electronic records management system (elektrooniline dokumentihaldussüsteem, EDHS), the electronic document management system (elektrooniline teavikuhaldussüsteem, ETHS) and the electronic document and records management system (elektrooniline teabehaldussüsteem)

In addition to managing records, electronic document and records management systems, abbreviated in English as EDRMS are often used to manage all the documents (mainly with unstructured content) created within the organisation; the systems draw a clear line between document management and records lifecycle management. As highlighted earlier, the terms document and record have to date been identically translated into Estonian as dokument. Due to this, the aforementioned systems have been introduced in Estonia as electronic records management systems or ERMSs (EDHS in Estonian), which primarily comprise the sub-modules of records management and records lifecycle management, respectively. This is a language-related source of ambiguity for users, which has also caused some confusion in the preparation of procurement documents. Due to this, clearly distinguishable terms have been used in the Estonian translation of MoReq2, including the terms teavik and dokument (as the equivalents of document and record, respectively) as well as teavikuhaldus and dokumentihaldus (document management and records management) and elektrooniline teavikuhaldussüsteem or ETHS and elektrooniline dokumentihaldussüsteem or EDHS (EDMS and ERMS).

As a rule, the records management systems commonly used in Estonia are used to manage records as well as some of the organisation’s documents, namely draft records. However, most documents and even some records are not included in ERMSs (instead, they can be found in e-mail applications, the file system of the operation system and in other information systems used in the organisation), and regrettably they are sometimes not considered to be a part of the organisation’s documents and records system and therefore do not receive the attention of the Records Manager. Among other things, this is a result of terminology confusion related to the concepts of records and documents.

Class, classification code, fully qualified classification code – sari, tähis, terviktähis

In English, there is a clear connection between the terms classification scheme, class and classification code used in MoReq2. The Estonian translation is based on terminology that is generally used in local records management and although liigitusskeem (see section 6.2) has been chosen as the translation equivalent for classification scheme, the other Estonian terms used for denoting related concepts do not originate from the same stem. Therefore, the term sari (in English: series) rather than liik (in English: class, type) is used in the Estonian translation of MoReq2 as an equivalent of the English term class; in the same vein,
the term tähis (in English: marker) rather than liigituskood (in English: classification code) is used as the equivalent of classification code.

Since the concept of class is used in MoReq2 to denote classes at any level of the classification scheme, it should be borne in mind when reading the Estonian translation of MoReq2 that the term sari also encompasses the levels of function, sub-function, sub-class and sub-sub-class (see section 6.2). In addition to the term classification code (in Estonian: tähis), MoReq2 also uses the term fully qualified classification code, which has been translated into Estonian as täielik tähis ehk viit. Here, the word viit is understood as a classification code attributed to a record or an aggregation that is formed by joining together the classification codes of the different levels of the hierarchy and which is unique within a classification scheme.

**Parent, child – ülenev/üleneja, alanev/alaneja**

Although in the field of information technology the term parent is often translated into Estonian as ema (mother) and the term child is translated as tütar (daughter), the Estonian translation of MoReq2 uses the terms alanev/alaneja (in English: descending/descendant) in the case of the child relationship and ülenev/üleneja (in English: ascending/ascendant) in regard to the parent relationship. This is based on analogy with the terminology of the Family Law Act and the desire to avoid the use of unsuitable compound words; therefore, parent class is translated as ülenev sari (ascendant class) rather than emasari (mother class), while child file is translated as alanev toimik (descendant file) rather than tütartoimik (daughter file). In cases where the words parent or child were not specified by a subsequent noun, they were translated as üleneja and alaneja, respectively.

A child of one entity (class, file, sub-file, volume) is located below it in the hierarchy; in other words, it is a descending entity. A parent of an entity is above it in the hierarchy; in other words, it is an ascending entity. Therefore, for example, descendants of one class can be other classes, i.e. sub-classes, files or records.

**Case management, case file – juhtumikorraldus, juhtumitoimik**

Case management information systems as described in MoReq2 are widely used in Estonia, although they are usually not known as such. After all, the term juhtumikorraldus (case management) is a relatively new one in Estonia and it is primarily used in the social sphere. The systems used for processing cases related to insurance, unemployment, probation supervision, incapacity for work, etc., are usually known in Estonia as principal activity information systems (põhitegevuse infosüsteemid), procedural systems (menetlussüsteemid) or business applications (ärikonkendused); in other cases, they are designated by the name or abbreviated name of the specific information system.

While case management/case work has been distinguished from the provision of a single assistance or service in Estonia 6, MoReq2 does not differentiate between these activities. Within the scope of MoReq2, the case files (juhtumitoimikud) managed in case management environments include various records that have been created in the course of predefined and often repeatable procedural processes and comprise several different types of records.

---

The implementation of MoReq2 in Estonia

(which can be stored in type-specific sub-files inside the file). This means that case files also include files related to assigning and paying various types of allowances, benefits, etc.; the types of case files discussed in MoReq2 also include files related to applications for permits, insurance policies, sale of land, etc. This approach is justified from the standpoint of records management, since the basic structure and management of the files is similar in all of the aforementioned cases. The term asja toimik has also been used in Estonian in the sense of a case file.

MoReq2 does not present requirements for case management information systems. However, the document does describe the required functionality of an ERMS integrated with a case management system. These requirements described in the MoReq2 are also highly relevant in Estonia.

Non-case file, file, sub-file, volume – tavatoimik, toimik, alltoimik, köide

The term non-case file used in MoReq2 has been translated into Estonian as tavatoimik and denotes any file (toimik) that is not a case file (juhtumitoimik).

Although physical or paper files often consist of volumes (köited), the term is not widely used in Estonia. Usually, a volume consists of the records of one administrative period (year, academic year, etc.); in some cases, large files are also divided into volumes based on their size (thickness), in order to facilitate their physical survival. In the case of electronic files, the division of files into volumes makes it easier to organise the disposition and destruction of records ("cut-off") as well as making it easier to find records when navigating through the classification scheme.

Sub-files (alltoimikud) are subdivisions of a file used mainly in case management; the records related to a case are divided into sub-files by type. This makes it possible to apply different retention and disposition schedules for records, depending on their type. In Estonia, sub-files have so far not been very common, although their implementation would be justified in the case of large personal files that are used over the course of long periods of time (e.g. pension files), since this would facilitate the disposal of records with short term relevance from the file and the data concerning those records from databases in a controlled manner once their retention period ends. However, sub-files can also be used in non-case files (e.g. structural aid files) in order to improve the organisation of records that are related to the same matter and have identical retention periods.

Vital records – esmatähtsad dokumendid

The concept of vital records (esmatähtsad dokumendid) is not generally used in Estonian records management practice. In MoReq2, the term is used for records that are extremely important for an organisation and must be the first to be recovered in the event of an emergency or a disaster. For this purpose, vital records are marked with indicators of their status and are subject to several separate back-up operations (for example, if back-up copies are made from all ERMS data once a week, vital records are backed up more frequently).

Vital records may be ephemeral (e.g. if the loss of the records may temporarily prevent an organisation from continuing its activities and/or hinder the provision of services) or may
require long-term storage (e.g. records with cultural or historical value or records that are necessary for protecting the interests of an organisation or individuals in the long term).

Although the concept of vital records is not widespread in Estonia, the same cannot be said for multistage backup. The changes made in an ERMS during the day are often backed up on a daily basis, while the entire database is backed up less frequently. At the same time, organisations should take the concept of vital records into consideration when establishing their backup routines. Vital records may include records and classes that have been found to have archival value as well as records which have not yet been fully processed (e.g. petitions by citizens, unanswered letters, unpaid invoices, etc.), or which are important as evidence of facts, activities, rights and obligations (e.g. contracts).

**Search, retrieval, presentation – otsimine/otsing, (otsingu tulemusel) leidmine, esitus**

While in the field of information technology the term *retrieval* is often used to denote an information retrieval (*infootsing*) that includes searching, finding and displaying (data or information), these concepts have been presented separately in MoReq2. This is important with regard to describing different functions and corresponds to everyday language use where a *search* indicates the process of looking for something, while *retrieval* points primarily to finding something (again), getting something (back) or delivering something. As a result, the Estonian translation of MoReq2 uses *otsimine* or *otsing* as the equivalents of the term *search*, *leidmine* or *kättesaamine* as the equivalents of the term *retrieval* and *esitus* as the equivalent of the term *presentation*. However, depending on the context, *retrieval* has been translated occasionally as *otsing*; for example, this is the case in requirement 8.1.24 where the phrase *in a single retrieval process* has been translated as *üheainsa otsingu käigus*.

In ERMSs, it is possible to search and retrieve files and records both by navigating through the classification scheme and by submitting enquiries to the system; once the files or records have been found, they can be presented either by displaying, printing or in other ways (e.g. in the case of audio files).

**Rendition, redaction – teisendkoopia and redaktsioon**

It is often necessary to make and retain copies of records in a file format that differs from the original. In MoReq2, such copies are referred to as *renditions* (*teisendkoopiad*) and their creation may be motivated by different reasons. For example, an incoming record may exist in a format that is not used by the organisation and may have to be rendered so that it could be processed. In the case of some records, it is necessary to retain an original copy over a long period (e.g. in PDF/A format) as well as an alterable copy that can be processed further (e.g. in DOC or ODT format), while in the case of other records it is necessary to have copies in a machine-readable format (e.g. XML) as well as a human-readable format (e.g. PDF).

In MoReq2, *redaction* (*redaktsioon*) refers to a copy of a record that has been *redacted* (*redigeeritud*) in order to mask or remove part of the information in the record without changing the meaning of its contents7. Records are redacted mainly in connection with the

---

7 The original MoReq used the term *extract* (*väljavõte*) instead of the term *redaction* (*redaktsioon*) and *väljavõte* was also used in the 2002 “Requirements” published by the Government Office. However, the term *väljavõte* (*extract*) has a different meaning in everyday language and therefore the Estonian translation of the MoReq2 term *redaction* (*redaktsioon*) corresponds to the original.
disclosure of information. In Estonia a lot of attention has been devoted to the disclosure of records (see section 6.5) and although the legislation does not make provisions for the disclosure of records containing sensitive information on an organisation's website, redacted copies of such records do have to be made available in case of a request for information.

The terms teisendkoopia and redaktsioon (as used in MoReq2 in the sense of rendition and redaction, respectively) are not commonly used in Estonia but are very important from the standpoint of understanding and implementing the requirements set forth in MoReq2. In addition to expanding our understanding, the adoption of these terms allows for the more accurate marking and linking of records and their copies in an ERMS. The transition of the Estonian public sector to using records in XML format (see section 6.4) will create new possibilities for preparing and disclosing redactions of records.

**Role, user role, administrative role – roll, kasutajaroll, administraatoriroll**

Although the term roll (role) is by no means unknown in Estonian, it is not used for referring to a person fulfilling a role. In MoReq2, however, the term role refers both to the set of functional permissions given to a user and to the person who makes use of those permissions. MoReq2 presents a system-based view, describing which activities an ERMS must permit or prevent with regard to users who have been assigned a specific role in the ERMS. Thus, the Estonian translation also uses constructions such as administraatoriroll peab saama valida, milliseid metaandmeid eksportida (an administrative role [must be] able to select which metadata is exported) (requirement 3.1.18) where the term administraatoriroll (administrative role) refers to a user of an ERMS who has been assigned the role of an administrator within the system. In order to maintain the clarity of linguistic expression, the terms kasutajaroll (user role) and administraatoriroll (administrative role) have been adopted as compound words. The use of the Estonian term haldur (administrator/manager) instead of the Latin-based term administraator (administrator) has been avoided to make the distinction between administraator and dokumentihaldur (records manager) clearer; in an organisation's ERMS, the administrative role can be assigned to a records officer, an archivist, a records manager as well as an IT specialist or an employee with another position title.

**Business (classification scheme, context, processes, needs, requirements, applications)**

The translation of the English term business into Estonian is complicated. Although the Estonian equivalent äri is a short and simple word, which can also easily be used to form compound words, it is understood outside the field of information technology mainly as commerce as well as a commercial enterprise, which differs from the intended meaning of MoReq2.

In MoReq2, the term business stands, in a certain sense, in contrast with both technology and records management; it is used to refer to an organisation per se (regardless of whether the organisation is a public sector institution or a privately owned company) and to the activities carried out to achieve the organisation's goals. As a result, the Estonian translation of the texts is mainly based on context: business classification scheme has been translated into Estonian as organisatsiooni tegevuste liigituse skeem (in English: classification scheme for an organisation's activities), business processes has been translated as tööprotsessid (in English: work processes), business sectors has been translated as majandusvaldkonnad (in
English: sectors of the economy), etc. However, the prefix äri- has been used in some phrases, especially in cases where it was necessary for avoiding complicated constructions or it corresponded to common language usage. Therefore, the phrase business needs has been translated as ärivajadused and business requirements has been translated as ärinõuded (or, in some contexts, also as ärivajadused), while the term ärirakendus, frequently used in the field of IT, has been adopted as the translation equivalent of business application. In the case of these terms, as was pointed out above, the interpretation of the word äri must not be limited to commerce and commercial enterprises.

Terms with parallel forms (check-out, check-in, on-line, off-line, near-line, pointer, webcasts, etc.)

The protection and development of the Estonian language is one of Estonia’s national policies. The increased use and development of the Estonian language is encouraged in all fields in order to ensure the continuity of Estonian language and culture. At the same time, Estonia also values multilingualism and openness. Information technology is one of the fields where English is often one of the working languages and where English terminology is widely used alongside Estonian terminology.

Based on these circumstances and the goal of ensuring the unambiguity of the requirements presented in MoReq2, the equivalent English terms have been added in parentheses after a number of Estonian terms in the text of the specification: veebilevi dokumendid (webcasts), kohavitt (pointer), vaatamistarkvara (viewer), etc. This is especially important in cases where the Estonian language lacks a generally accepted equivalent for a term, such as in the case of the terms check out and check in. In MoReq2, the latter have been translated into Estonian based on their substance: check-out is translated as EDHSis väljavõetuks märkimine (marking as having been checked out from the ERMS) and check-in is translated as EDHSi tagastatuds märkimine (marking as having been returned to the ERMS); when the same terms are repeated within the same context, simplified forms like väljavõtmine and tagastamine have been used.

It should be noted that the English equivalent of a term is usually provided only once per section and only the Estonian translation is provided when the term is repeated within the same section.

2.5 Estonian chapter zero

The MoReq2 allows member states of the European Union to describe their specific national requirements in a so-called chapter zero. This chapter zero contains information on which national requirements and solutions must be taken into consideration when implementing MoReq2 in Estonia. Most of the requirements described in the chapter apply primarily to public sector institutions, although private sector companies have also followed the requirements in acquiring and developing their ERMSs.

The first version of the Estonian chapter zero was prepared by the Records Management Department of the Government Office. The following parties were involved in the process of preparing the Estonian chapter zero: AS Fujitsu Services, lecturers on the speciality of

---

8 The project for creating the Estonian chapter zero was led by Kädi Riismaa (the Government Office).
The implementation of MoReq2 in Estonia records management from Tallinn University and the University of Tartu Viljandi Culture Academy as well as specialists from the National Archives, the Department of State Information Systems of the Ministry of Economic Affairs and Communications, the Estonian Informatics Centre (as of 1 June 2011 Estonian Information System’s Authority) and the Certification Centre. The Estonian chapter zero was published together with the Estonian translation of MoReq2, but as a separate document.

The chapter zero was updated in 2012 by the Department of Information Society Services Development of the Ministry of Economic Affairs and Communications, taking also into account the suggestions of the National Archives and the Estonian Information System’s Authority.

The Estonian chapter zero has been prepared with readers from Estonia as well as other countries in mind; it has been translated into English and validated by the MGB. The Estonian chapter zero was translated into English by Wiedemannü Translation Company. The validation of the chapter zero was carried out by Marko Lukić as the representative of the MGB. The amendments to the chapter zero were validated by Aleksandra Mrdavšić as Accessibility Convenor.

2.6 Publication of the translation of MoReq2 and chapter zero

The Estonian translation of MoReq2 and the Estonian chapter zero are published on the basis of license agreement no. LP-005-ET, agreed between the Secretariat-General of the European Commission and the Government Office and handed over to the Ministry of Economic Affairs and Communications. The translation and the chapter zero are available via the DLM-Forum website at [http://www.dlmforum.eu](http://www.dlmforum.eu/).

The translation and the chapter zero have been prepared using the word processing software Microsoft Word 2003 and published in the Adobe PDF format.

9 The Estonian chapter zero was translated into English by Wiedemannü Translation Company. The validation of the chapter zero was carried out by Marko Lukić as the representative of the MGB. The amendments to the chapter zero were validated by Aleksandra Mrdavšić as Accessibility Convenor.
3 ESTONIAN NATIONAL CHARACTERISTICS: DEVELOPMENT OF RECORDS MANAGEMENT AND THE REGULATORY ENVIRONMENT

3.1 The organisation of records management in Estonia

In accordance with the Government of the Republic Act and the Statutes of the Ministry of Economic Affairs and Communications, the development of state information systems, public services, and from 2012 onwards also records management is coordinated by the Ministry of Economic Affairs and Communications.

The Ministry is assisted by the Records Management Board, which comprises, in addition to the coordinators of the aforementioned fields, records management officers of the ministries and the Government Office, as well as representatives of the developers of records management in local governments, the National Archives, and the Estonian Information System's Authority.

The principles of coordinating the development of records management are stipulated in more detail in the regulation of the Government of the Republic on the Common Principles of Administrative and Records Management Procedures.

The retention of records with archival value that have been created in the process of performing public duties is organised by the National Archives of Estonia and the development of the state information system is organised by the Estonian Information System’s Authority. The Estonian Information System’s Authority is governed by the Ministry of Economic Affairs and Communications; from 2012 onwards, the National Archives is governed by the Ministry of Education and Research.

Additional information:

- *Vabariigi Valitsuse seadus* (Government of the Republic Act) – available via Riigi Teataja (see section 3.2)
- *Majandus- ja Kommunikatsiooniministeeriumi põhimäärus* (Statutes of the Ministry of Economic Affairs and Communications) – available via Riigi Teataja (see section 3.2)
- National Archives website: [http://www.ra.ee/](http://www.ra.ee/)
- Estonian Information System's Authority website: [http://www.ria.ee/](http://www.ria.ee/)
3.2 Legislation, standards and guideline that apply to the field

*Riigi Teataja*

Estonian legislation is published in the official state gazette Riigi Teataja, which has been issued solely in electronic form since 2010. Riigi Teataja is available online for free and can be used to access all of the laws and regulations referenced in this chapter. Since Riigi Teataja is the official online publication of the Republic of Estonia, the texts and data published therein are legally binding. In addition to legislation, Riigi Teataja also publishes other legal instruments and in the future will also provide access to explanatory memoranda to legislation, decisions of the Supreme Court and other documents and data connected to legal instruments. It is possible to subscribe to reports regarding the amendment of legislation published in Riigi Teataja, which will be sent to the subscriber’s e-mail address.

Selected legislation is translated into foreign languages; the translation process and the publication of the translations are handled by the Ministry of Justice. As of 2011, the translations are published in Riigi Teataja, while the earlier translations can be found on the Ministry of Justice website. In the case of the latter, it is useful to bear in mind that newer redactions of translated legislation may exist.

*Laws*

Estonia currently lacks a law that would regulate records management in a comprehensive and uniform manner. As a result, it is necessary to use many laws that regulate different aspects of records management. Public sector institutions, first and foremost, must take the following legislation into account when organising their records management:

- **Avaliku teabe seadus** (Public Information Act), which provides the conditions of, procedure for and methods of accessing public information (including the procedure for maintaining registers of records), the bases for establishing and managing databases and the supervision of the organisation of database management and the provision of access to information.
- **Isikuandmete kaitse seadus** (Personal Data Protection Act), which provides the conditions and procedure for processing personal data, the procedure for state supervision over the processing of personal data and the liability for violation of the personal data processing requirements.
- **Märgukirjale ja selgitustaotlusele vastamise seadus** (Response to Memoranda and Requests for Explanations Act), which provides the procedure for responding to inquiries presented by persons.
- **Arhiiviseadus** (Archives Act), which provides for the organisation of appraisal of records, acquisition, preservation and accessing of archival records, and the bases of the activities of public archives.
- **Digitaalallkirja seadus** (Digital Signatures Act), which provides the necessary conditions for using digital signatures and digital stamps and the procedure for exercising supervision over the provision of certification services and time-stamping services.

---

10 It should also be noted that, as with Estonian language, the term *document* is often used in the meaning of *record* in the earlier translations.
• *Haldusmenetluse seadus* (Administrative Procedure Act), which is aimed at ensuring the protection of the rights of persons through the creation of a uniform procedure and which allows for the participation of persons and judicial control.

• *Riigisaladuse ja salastatud välisteabe seadus* (State Secrets and Classified Information of Foreign States Act), which provides the bases of classification, changing the classification, the procedure for the protection of classified media and the liability incurring from violation of the act.

• other laws that establish specific conditions for the creation, retention or use of records (personnel and accounting records, etc.) by specific organisations, (e.g. Perioodi 2007-2013 struktuuritoetuse seadus (2007-2013 Structural Assistance Act), which regulates the retention of records related to the provision and use of assistance).

**Regulations of the Government of the Republic**

The following two regulations of the Government of the Republic are especially important with regard to introducing and developing an organisation’s records system:

• “Asjaajamiskorra ühtsed alused” (Common Principles of Administrative and Records Management Procedures), which regulates the records management of state and local government institutions and legal persons in public law, the creation, registration, processing, signing and keeping of records and provides general requirements for records management systems, records registers and the exchange of records between organisations.

• “Arhiivieeskiri” (Archival Rules), which contains a more detailed set of guidelines for carrying out the tasks set forth in the Archives Act. Among other things, the regulation establishes the formats to be used for long term preservation, which must be followed when creating and managing digital records with long retention periods, including digital records with archival value.

**Ministerial regulations and directives**

Ministerial regulations or directives may regulate:

• records management in certain institutions belonging to an area of government (e.g. Minister of Justice regulation no. 23 of 19 June 2009: “Notariaadimäärustik” (Notaries Regulation));

• records management in all institutions belonging to an area of government (e.g. Minister of Social Affairs regulation no. 56 of 18 September 2008 ”Tervishoiuteenuste osutamise dokumenteerimise ning nende dokumentide säilitamise tingimused ja kord” (Conditions and Procedure for Maintaining Records of the Provision of Healthcare Services)).

**Standards**

The standards that apply to the field of records management can be divided into four groups: (1) system and process standards, (2) metadata and description standards (3) structure and form standards for document types and (4) format standards for digital documents. Various technical standards concerning office work are also implemented in the field of records.
Although standards are considered to be voluntary agreements in Estonia, it is possible to make certain standards compulsory for the public sector through legislation. For example, institutions are obligated to implement the international archival description standard (ISAD(G)) with regard to describing archives. In Estonia, records management standards have mainly been transposed from the standards of the International Organization for Standardization (ISO), although some original Estonian standards have been established for the field. Several information technology standards are also used in electronic records management, such as the web standards recommended by the World Wide Web Consortium W3C (www.w3.org). While the web standards can generally be distributed freely and at no charge, the rights of distribution of other standards can be restricted. The Estonian Centre for Standardisation is the standards organisation that prepares, publishes and distributes Estonian standards; the Centre’s technical committee, EVS TK-22, is responsible for the field of information and documentation.

The following international standards have been transposed as Estonian standards:

- EVS-ISO 5127:2004 "Information and documentation - Vocabulary";
- EVS-ISO 15836:2011 "Information and documentation - The Dublin Core Metadata Element Set";

Original Estonian standards and guidelines:

- EVS GUIDELINES 9:2006 "Dublin Core'i metaandmeelementide kasutamine“ (Use of the Dublin Core metadata elements) provide a more thorough description of the Dublin Core element qualifiers and the use of the Dublin Core element set in describing information resources;
- EVS 8:2008 “Infotehnoloogia reeglid eesti keele ja kultuuri keskkonnas“ (Requirements of information technology in Estonian language and cultural environment). The standard provides information on Estonian language locale for

---

11 The most recent information on the Estonian records management standards is available on the National Library of Estonia website at www.nlib.ee.
Estonia and narrative cultural specifications, and includes code tables and correlation tables.

**Guidelines, good practice and best practice**

Various guidelines can be helpful in the course of creating and developing a records system:

- Ministry of Economic Affairs and Communications’ guidelines\(^{12}\), the emphasis of which is mainly on harmonisation of administrative procedures and records management in the public sector, enhancement of interoperability between ERMSs and promotion of electronic records exchange: “Dokumendihalduse metaanndmete loend” (Records Management Metadata Set), “Dokumendiligi XML andmekirjelduse koostamine” (Developing an XML Data Description of a Record Type);
- National Archives’ guidelines for organising records and archive management, which focus mainly on the aspects of long-term preservation of records.

An organisation’s internal regulations for records management (the records management procedure, the list of record classes described in section 6.2) must reflect the conformity of the organisation’s records management and administration with the legislation in force and the accordance of these processes with the applicable standards, good practice and best practice. For this purpose, references to legislation of general application are included in the public sector institutions’ internal regulations and rules on records management.

**Additional information:**

- Riigi Teataja: [http://www.riigiteataja.ee](http://www.riigiteataja.ee)
- Selection of translations of laws into English: [http://www.just.ee/6906](http://www.just.ee/6906)
- Estonian Centre for Standardisation: [http://www.evs.ee/](http://www.evs.ee/)

---

\(^{12}\) The guidelines by the Government Office are to be followed until the guidelines by the Ministry of Economic Affairs and Communications have been issued.
4 ESTONIAN NATIONAL CHARACTERISTICS: ERMSs AS A PART OF THE STATE INFORMATION SYSTEM

4.1 Development of information society, the interoperability framework and paperless administration

Since 2006, the Government of the Republic has been on a course towards paperless administration in the public sector. In order to achieve this goal, a system for exchanging electronic records between government institutions through the X-Road Document Exchange Centre (hereinafter “DEC”, see section 4.5) has been established and an XML repository (see section 4.3) has been created for the purpose of facilitating the implementation of XML-based records in accordance with the “Estonian Information Society Strategy 2013” adopted by the Government of the Republic and the operational programmes based on the strategy.

The Department of State Information Systems (RISO) of the Ministry of Economic Affairs and Communications has prepared a strategy document entitled “Estonian IT Interoperability Framework”, which covers the most general principles related to the country’s IT interoperability and is intended to be followed in developing and managing information systems at the level of the state and local governments. The framework consists of field-specific instalments; a “Records Management Interoperability Framework” is under development and will describe the most important aspects related to creating an interoperable records management system.

Additional information:


4.2 State information system

The development of the state information system that supports the provision of public services in Estonia is based on the principles of dispersed development. Dispersed development requires the use of the Open Method of Coordination. According to this method, the parties involved agree on a set of minimum requirements that, if followed, ensure the technological interoperability of information systems and the semantic interoperability of data. The development and management of the state information system is coordinated by RISO.
Important bases for Estonian IT architecture include interoperability, security, openness, flexibility and scalability. The IT architecture is based on the principles of service-oriented architecture (SOA). Various systems provide different information services through so-called "service interfaces", which are accessible to other information systems. The descriptions of the interfaces must contain sufficient information to allow the service to be identified and used without the system using the service having to "know" anything about the internal architecture, platform, etc. of the system that is providing the service. The technologies used for implementing a service-oriented architecture are not limited and the publisher of the service and the actual service provider may be different entities.

An infrastructure service is a common set of operating rules or technical functionality used for providing one or several services or managing an information system. Effective infrastructure services ensure that the state information systems function as a uniform whole. Some infrastructure services – support systems – are provided for in the Public Information Act and the regulations based thereon. The use of support systems is obligatory for maintaining state and local government databases. There are currently six support systems:

- the classifications system;
- the system of security measures for information systems (ISKE);
- the address data system;
- the data exchange layer of information systems (X-Road);
- the geodetic system;
- the administration system of state information system (RIHA).

Joint infrastructure services, including support systems, are executed in a centralised fashion and are free for everybody. The services can be used as building blocks for creating architecture for your information systems or as tools for realising functionality. The number and composition of joint infrastructure services changes over time. Three of the services are described below.

**Additional information:**

- *Avaliku teabe seadus* (Public Information Act)
- Regulation of the Government of the Republic "Klassifikaatorite süsteem" (Classifications System)
- Regulation of the Government of the Republic "Infosüsteemide turvameetmete süsteem" (System of Security Measures for Information Systems)
- Regulation of the Government of the Republic "Aadressiandmete süsteem" (Address Data System)
- Regulation of the Government of the Republic "Infosüsteemide andmevahetuskiht" (Data Exchange Layer of Information Systems)
- Regulation of the Government of the Republic "Geodeetiline süsteem" (Geodetic System)
- Regulation of the Government of the Republic "Riigi infosüsteemi haldussüsteem" (Administration System of State Information System)
4.3 Administration system of state information system (RIHA) and its components

The administration system of state information system (RIHA) is a complete and detailed catalogue of the state information system. RIHA consists of administration principles and an information system that supports these principles and is located at https://riha.eesti.ee.

The goal of RIHA is to ensure the administration and transparency of the state information system, planning the state's information management, and supporting the interoperability of the databases of the state, local governments and private persons that perform public duties. RIHA administers information systems, services, and classifications of the state, as well as semantic and XML assets. For the most part, RIHA's data is available to everyone, but can be amended only by the organisations registered in RIHA; each organisation is individually responsible for the correctness of the data they have entered.

In accordance with the Public Information Act, all databases – including ERMSs – that are operated by the state, by local governments or other legal persons performing public duties have to be registered in RIHA. Since ERMSs are, as a rule, standardised products that are used by several different organisations in versions that have been customised to varying degrees, RIHA registers both the standard solution and its users. Databases with restricted access arising from the State Secrets and Classified Information of Foreign States Act are not registered in RIHA.

The regulation of the Government of the Republic on the Common Principles of Administrative and Records Management Procedures sets forth requirements for the electronic exchange of records. In accordance with the regulation, data descriptions are registered in the RIHA XML repository on all types of records transmitted via the X-Road Document Exchange Centre (DEC). The descriptions of standard elements and containers used in the exchange of electronic records and data, standard metadata sets and schemes, and other XML assets are also registered in the repository. The purpose of the XML repository is to support the reuse of XML assets and increase the interoperability of different systems.

Additional information:

- **Avaliku teabe seadus** (Public Information Act), Chapter 51 “Andmekogud” (Databases)

- Regulation of the Government of the Republic “Riigi infosüsteemi haldussüsteem” (Administration System of State Information System)
• Regulation of the Government of the Republic “Asjaajamiskorra ühtsed alused” (Common Principles of Administrative and Records Management Procedures)
• RIHA: http://www.ria.ee/27313

4.4 Information systems’ data exchange layer X-Road and the State Portal

X-Road is a data exchange layer created for Estonia’s state information systems; it allows citizens as well as officials and entrepreneurs to securely use a large share of Estonia’s databases online. For example, every citizen can use X-Road to submit inquiries to the Population Register about their personal data or inquiries to the vehicle database of the Traffic Register regarding their car.

In addition, X-Road provides the opportunity to form connections between different databases, thereby making it possible to use the data from other information systems in an ERMS or to use the data from an ERMS in other information systems. X-Road mainly uses the SOAP protocol for exchanging data and a secure connection is created between two parties through standard security servers in order to ensure the safety of the data exchange. In the data exchange, a two-step authorisation is used – an agency is authorised in the security server of X-Road, and a user is authorised in the information system of the agency. Web services attached to X-Road are described in the standard WSDL format.
The implementation of MoReq2 in Estonia

Figure 2. X-Road and ERMSs

The X-Road infrastructure is also used by the Estonian information gateway, the State Portal eesti.ee, which has been designed for use by citizens as well as entrepreneurs and officials. The portal brings together many of the information systems that are in use in Estonia and provides its users with the opportunity to find the necessary information and gain access to various X-Road, register and information system services through one portal. On the opening page of the portal, a user can choose whether to use e-services, read materials on various topics, or search for contact data of agencies. After choosing e-services or topics, a choice can be made whether to search further in the area designed for citizens, entrepreneurs or officials and, depending on the user’s choice, the list of services or topics intended for the role in question can be retrieved.

All of the inquiries made through X-Road possess probative value, i.e. have a legal effect. This means that inquiries made through X-Road can later be identified along with the person who submitted the inquiry and it is possible to establish that the inquiry has been logged correctly.

Additional information:

- Regulation of the Government of the Republic “Infosüsteemide andmevahetuskiht” (Data Exchange Layer of Information Systems)
- Data Exchange Layer X-Road, 2007: http://www.ria.ee/indexphid27309
- X-Road guidelines: http://www.ria.ee/x-tee-juhendid/
- State Portal: http://www.eesti.ee

4.5 Document Exchange Centre (DEC)

In addition to traditional records exchange methods, the Document Exchange Centre (DEC) which functions through the X-Road is widely used by Estonia’s public sector institutions; its operating principles are shown in the following figure.
The implementation of MoReq2 in Estonia

Figure 3. Structure of the DEC

The goal of the DEC is to connect distant ERMSs for the secure transfer of records and, in the near future, to provide services that support the processing of records. Exchanging electronic records through the DEC is compulsory for all government authorities. In addition, more than 500 bodies and organisations have voluntarily joined the DEC (an actively updated list of the organisations is available at http://www.eesti.ee/portaal/dvk.asutused).

In order to use the DEC, each communication partner must have a DEC account and each organisation communicating with the DEC must have an X-Road security server for creating a secure connection. Technical interconnection with the DEC is possible through the DEC universal client interface offered by the Estonian Information System’s Authority and the DEC Java API. In order to ensure problem-free records exchange, an organisation joins the DEC production environment only when its ERMS is completely prepared for receiving and sending records through the DEC. The DEC test environment must be used when testing the interface and the records exchange process.

Since the number of DEC users is constantly increasing, the ERMSs contact the DEC at least once daily to download the latest list of users. This allows for the automatic sending out of records: DEC is automatically appointed as the method of transfer of the records if the addressee is on the list of organisations that have joined the DEC.

Records are transferred in SOAP envelopes with XML containers (“envelopes” of records) each of which, in turn, contains a record and an extract of its metadata. The transfer of a standard metadata set facilitates the capturing and registration of the records in the recipient’s system, since the necessary metadata can be populated automatically.
Instead of passing on the records that arrive at the DEC central server, the server waits for the communication partner itself to ask for the newly arrived records. This helps to avoid the loss of records that may occur in the case of other means of records transfer, such as e-mail. Upon the arrival of the records, the recipient’s system returns the appropriate confirmation. Furthermore, authorised employees of an organisation that has joined the DEC can use the DEC reporting module for searching and viewing records sent and received by the organisation, grouping the records on the basis of various criteria (e.g. sending time, status, sender, recipient) and preparing reports based on this information.

Since the DEC data exchange takes place over the secure X-Road, the authentication and authorisation of the senders and recipients of records is done automatically with the help of the X-Road security servers. Citizens and companies can exchange records with organisations that have joined the DEC and monitor the course of the processing of the records through the mediation of the Official Records Infrastructure Service (ADIT), which has been created for the State Portal eesti.ee. The e-invoices of private companies are transferred by the DEC to organisations through operators that handle private sector settlements or through a new service “Create an e-invoice” of the State Portal. The DEC can also be used for the purpose of exchanging records and the data thereof between ERMSs and other organisational or inter-organisational information systems (for example, legislation is sent to Riigi Teataja for publication through the DEC).

**Additional information:**


- DEC: [http://www.ria.ee/dec](http://www.ria.ee/dec)

• Description of the DEC reporting module: http://www.ria.ee/dvk-aruandlusmoodul

• Description of the ADIT service: http://www.ria.ee/ametlikud-dokumendid
5 ESTONIAN NATIONAL CHARACTERISTICS: E-IDENTITY AND INFORMATION SECURITY

5.1 Estonian personal identification code and digital identity documents

Estonia has created several methods for personal identification and identity checking in an electronic environment. These methods make it possible to authenticate and authorise persons in information systems, digitally sign and encrypt records or link persons with specific records or data.

**Estonian personal identification code**

In ERMSs, personal identification codes are often used to identify which records, the processes related thereto, and other activities and objects are connected with a person. Personal identification codes are also stored in the chips of digital identity documents.

Personal identification codes are unique 11-digit identifiers issued to individuals registered in the Estonian Population Register. The numerical combination issued as a personal identification code includes the individual’s date of birth, gender, serial number and a check digit. The latter allows for the detection of mistakes made in entering a personal identification code.

**ID cards and residence permit cards**

An identity card or ID card is an obligatory identity document for Estonian or EU citizens who reside in Estonia permanently. A residence permit card is the identity document issued to aliens who reside in Estonia permanently. The ID card and the residence permit card allow individuals to authenticate themselves in information systems, give digital signatures and encrypt data. The ID card can also be used as a travel document within the borders of the European Union.

Both the ID card and the residence permit card contain two certificates. One certificate is intended for establishing an individual’s identity and the other is used for issuing digital signatures. Each card holder is also automatically provided with an e-mail address ending with @eesti.ee. An ID card reader and the appropriate software are needed to use the cards.

**Digi-ID and Mobile ID**

A person can also use a digital identity card or Digi-ID to be identified digitally and give digital signatures. This can be necessary in the circumstances when it is impossible or unwanted to use an ID card for performing one’s duties at work (e.g. in order to prevent the spread of infection at hospitals, or to avoid damaging the ID card when used intensively). Unlike an ID card or a residence permit card, a Digi-ID does not contain a photograph of its owner which means that it cannot be used as a visual identity document.
One form of a digital identity card is the Mobile ID, which can be used for digital identification and giving digital signatures via a mobile telephone. A SIM card capable of handling the service is required in order to apply for a Mobile ID. Before a Mobile ID can be used, the holder of the ID has to activate it using an ID card or a residence permit card; after this, the person will be able to use the Mobile ID to authenticate themselves and digitally sign documents. Just as with other types of identity cards, the aforementioned activities are protected with security technology and PIN codes. The difference lies in the fact that the Mobile ID can be used without a separate card reader and the computer software necessary for using the reader.

Additional information:

- Rahvastikuregistri seadus (Population Register Act)
- Isikut tõendavate dokumentide seadus (Identity Documents Act)
- Identity documents: http://www.politsei.ee/en/ (Services)
- Estonian ID Portal: http://www.id.ee
- Certification: http://www.sk.ee

### 5.2 Estonian digital signatures and stamps; authentication and encryption

If the certificates of an ID card, a residence permit card or a digital identity card are valid, the card holder can authenticate themselves in information systems and provide records with digital signatures as well as encrypt and decrypt them. The authority of a signatory and the authenticity of records can be confirmed by an organisation with a digital stamp.

The use of digital signatures and stamps in organisations is regulated by the Digital Signatures Act, the Administrative Procedure Act and the regulation of the Government of the Republic on the Common Principles of Administrative and Records Management Procedures, as well as several field-specific pieces of legislation; authentication in ERMSs is discussed in the Common Principles of Administrative and Records Management Procedures. Organisations establish their detailed rules regarding authentication and the use of digital signatures and stamps in legal instruments that regulate their internal organisation of work (operations procedure, procedure for using the ERMS, procedure for the registration of records, etc.).

**Authentication**
In addition to the traditional form of authentication with a username and password, Estonia’s information systems are increasingly using an even safer method of authentication: the authentication of users with the help of an ID card. Instead of the ID card, a Mobile ID or Digi-ID as well as a residence permit card can be used for the purposes of authentication. As of 2011, this certificate-based method of authentication can even be mandatory in the case of public services that are provided electronically.\footnote{See the Identity Documents Act}

ID cards and other digital identity documents (e.g. the Mobile ID) are also used more and more to log into ERMSs and it is necessary for an ERMS to support this method of authentication.

**Digital signatures**

Directive 1999/93/EC of the European Parliament and of the Council (on a Community framework for electronic signatures) establishes the requirements for electronic signatures and certification service providers. The directive describes several categories of certification and electronic signatures. Estonian digital signatures, digital identity documents, and certification and time stamping services correspond to the directive’s categories with the most stringent requirements (i.e. advanced electronic signature, secure signature-creation device, qualified certificate, certification-service-provider issuing qualified certificates). The nature of the Estonian digital signature is governed by the Digital Signatures Act and it is legally equivalent to a manual signature.

Estonian digital signatures are calculated mathematically based on the document hash and the secret key protected with PIN code, and retained in the data field of the DigiDoc container. A DigiDoc container is an XML package containing the signed file, the signature and its mandatory attachments, presented in the DDOC file format. In Estonia, the free application software DigiDoc Client is widely used for managing DigiDoc containers (for signing, checking the signature, encrypting, decrypting). The software also has a web-based counterpart.\footnote{See the DigiDoc portal}

At the time when a digital signature is given, the digital signature software also checks the validity of the certificate used for signing. If the certificate can be used to sign a document, the confirmation of validity and the certificate of the institution that confirmed the validity will be recorded in the DigiDoc container as attachments of the signature. If a document is signed by several persons, every signature with its verification data will be recorded in the container. In the case of a negative result (i.e. the certificate is not valid), the signing process will fail and a signature will not be added to the document.

When the signature is checked at a later date, it is not necessary for the certificate used in the signing process to be valid: the information in the DigiDoc container will confirm that the signatory had the right to give the signature at the time. Also, it is not necessary to be connected to the Internet in order to check the signature – having the DigiDoc container management application will suffice. When records in DigiDoc containers are captured into an ERMS, it is usually not necessary for the details related to checking the signature to be duplicated in the records’ metadata.
The implementation of MoReq2 in Estonia

The current ID card base software supports both the DigiDoc XML format and the ZIP-format BDOC containers. The format of the BDOC container described in the Estonian standard EVS 821:2009 is based on the file structure described in the Open Document Format standard and supports stronger algorithms such as SHA256 (SHA2).

The ERMSs used in Estonia must allow the users to open records bearing Estonian digital signatures and it is also recommended that users be allowed to sign records without leaving the ERMS (see also section 6.1). Multiple individuals must be able to sign a record, if necessary.

When a document is signed digitally, its component(s) is/are “locked” and can no longer be altered; this also means that it is impossible to add information created during the registration process (e.g. classification code, date). As a result, in practice to date, automatic routines have been created that carry out the following steps of a single process when records are digitally signed in the ERMS:

- the automatic registration of a record is activated prior to the signing,
- in the course of which a fully-qualified classification code is allocated to the record; this code and the registration date are entered into the contents and metadata of the record,
- the record is converted to a file format suitable for long term preservation and
- the record is signed and stored in the ERMS as a .ddoc file.

In the case of two or more signatures, the records are already locked after the first signing. This fact must be taken into account when developing internal operating procedures for an organisation.

**Digital stamps**

Unlike digital signatures given with an ID card, digital stamps are digital confirmations provided by legal persons. Sertifitseerimiskeskus (the Certification Centre) will issue one or several certificates for the use of a digital stamp. Different certificates can be used for different purposes.

The digital stamp is intended as a substitute for a regular stamp, seal or impression of a seal and can be used both alongside a personal digital signature and separately. Digital stamps can be used to confirm the authenticity of copies, to confirm the authorisation of the person providing a digital signature, etc. Stamps can also be generated automatically: for example, on extracts made from information systems, on e-invoices, etc. Individual records or files can be confirmed with a digital stamp with the help of the DigiDoc software, while the TempelPlus software has been developed for the purpose of providing large numbers of records with digital stamps.

Digitally stamped records can be opened with the DigiDoc software. Just as in the case of digital signatures, the data on issuing and verifying the digital stamp are recorded in the DigiDoc container. If records are sent out with a digital stamp, the addressee can check whether the records have been sent by the right organisation or ascertain whether the person who signed the records was authorised to act as a signatory on behalf of the organisation. This allows the addressee to be certain that the records sent to them have not been amended.
**Encryption**

Encryption using the Estonian ID card, residence permit card or digital identity card is primarily intended to enable users to securely transfer records and single files containing sensitive information over an unsecured data communication channel (e.g. by e-mail). When encrypting the files, the user specifies the persons who have the right to decrypt them. This can be accomplished with the help of the card holders’ public certificate directory (LDAP directory service)\(^\text{15}\). Since the encrypted files can only be opened by certificate holders who have been listed as addressees, the encrypting user must not forget to add themselves to the list of addressees if they might have to open the file later.

The DigiDoc Crypto application software is used for encrypting and decrypting with an ID card, a residence permit card or a digital identity card; the Mobile ID does not support encryption and decryption. The certificates for the Digi-ID chip and ID card are different, meaning that when the Digi-ID is used for encrypting data, the data cannot be decrypted with an ID card and vice versa.

In order to decrypt data, the user needs a secret key that corresponds to the public key included in the authentication certificate and is ONLY available on the user’s ID card or other digital identity document. The secret keys connected with the certificates of digital identity documents cannot be moved outside of the chip of the card and therefore no backup copies of the keys can be made. If an identity document becomes unusable or the certificate transferred to the document becomes invalid (e.g. when the period of validity expires or a new card is issued), the user can no longer open the records or files encrypted with the card earlier and no other individual than those listed as addressees can open them. All of the aforementioned circumstances have to be taken into account with regard to capturing and managing encrypted records in an ERMS; it is not recommended to store records in encrypted form if they have to be retained over a long period. Archives also refuse to accept encrypted records.

In Estonia, there is a secure records exchange environment – the DEC – which can mostly be used to transfer records without encrypting them. The management, encryption and exchange of classified information are regulated by the State Secrets and Classified Information of Foreign States Act and the legislation based thereon.

**Additional information:**

- *Isikut tõendavate dokumendite seadus* (Identity Documents Act)
- *Digitaallallkirja seadus* (Digital Signatures Act)
- *Haldusmenetluse seadus* (Administrative Procedure Act)

\(^{15}\) LDAP directory service is one of the validity services provided by the Certification Centre.
The implementation of MoReq2 in Estonia

- Standard EVS 821:2009 “BDOC. Digitaalallkirja vorming” (BDOC. Digital Signature Format)


- Configuration of web servers for ID card-based authentication http://www.id.ee/?id=11020

- DigiDoc software: https://installer.id.ee/

- DigiDoc portal: https://digidoc.sk.ee/

- Encryption: http://www.id.ee/11114

- Certification Centre: http://www.sk.ee

- TempelPlus software: http://www.sk.ee/teenused/digitempli-teenus/tempelplus/

5.3 ISKE: a three-level baseline security system for information systems

In order to ensure the security of information systems and assets, Estonia uses ISKE, a three-level baseline security system that is implemented in accordance with the regulation of the Government of the Republic on the System of Security Measures for Information Systems. The implementation of ISKE is compulsory for ensuring the security of information systems used in maintaining state and local government databases and the information assets related to those systems, although private companies can also implement ISKE.

A security class is the level of security required for the data in question, which depends on the importance of the data and is assigned to each database and information system on the basis of the ISKE implementation guide. In order to determine the security class, an organisation conducts analysis and decides which availability, integrity and confidentiality levels are appropriate for the data in the information system. The security class is used to determine the necessary protection level from ISKE’s three levels: low (L), medium (M) or high (H). An analysis also has to be conducted regarding an ERMS in order to determine the level of security required for protecting its data and to implement the corresponding ISKE security measures. ISKE is taken into account both in the case of describing the requirements established for the ERMS (regarding authentication, data backup and recovery, the availability and scalability of the system, etc.) and concluding service level agreements (SLAs) with external service providers.

ISKE has been developed on the basis of a baseline security system used in Germany. ISKE contains a directory of hazards that lists a number of familiar risks as well as a directory of security measures that defines the methods for eliminating the hazards. In order to fulfil the ISKE requirements, the security measures described must be adopted on the basis of the security level of the information system. The set of measures has been presented in a
layered format, meaning that the middle level is achieved by adding certain measures to the lower level and the high level is achieved by adding certain measures to the middle level.

**Additional information:**

- Regulation of the Government of the Republic “Infosüsteemide turvameetmete süsteem” (System of Security Measures for Information Systems)


6 ESTONIAN NATIONAL CHARACTERISTICS: NATIONAL REQUIREMENTS FOR ERMSs

6.1 Main requirements for ERMSs as outlined in legislation

The Regulation of the Government of the Republic on the Common Principles of Administrative and Records Management Procedures establishes the most important obligatory requirements for ERMSs. Most of them can be met by implementing the MoReq2 requirements.

One ERMS can be used for records management by several institutions if the ERMS allows them to simultaneously use different and independent classification systems for classifying records. Therefore, an ERMS should support the use of several classification schemes.

ERMSs as inter-organisational or organisational electronic information systems used for creating, managing and processing records must ensure the adequacy of administration and records management, and allow for:

1) registration of records, regardless of their medium;
2) use of provided access privileges;
3) easy and quick access to records;
4) records management and archival transactions both with regard to individual records and aggregations of records;
5) the compilation and retention of records in a way that ensures the authenticity, reliability, integrity and usability until they are disposed for destruction or transfer to an archive;
6) the identification, at any time, of the transactions performed in the system, the time of the transactions and the persons who performed them.

Additional requirements have been established for the ERMSs of ministries, the Government Office, county governments, executive agencies and inspectorates which, in addition to meeting the requirements listed above, must allow:

- records to be approved, signed and transmitted;
- records to be automatically linked to metadata that describe the context, contents, structure and management history of the records;
- records to be sent and received through the DEC.

It is recommended that all other public sector institutions also follow the additional requirements.

6.2 Classification scheme and list of record classes

Like MoReq2, the Estonian chapter zero recommends that the public sector use a classification scheme based on the functions of the organisation, which will present a multi-level (hierarchical) overview of the organisation’s functions, activities and the records
documenting them. Classification schemes have to be developed in accordance with the requirements of the Government regulation “Arhiivieskiri” (Archival Rules).

The functions of an organisation are conventionally divided into executive, primary and support functions. Primary functions are the duties assigned to the organisation by law and/or in its statutes, which are based on the purpose of the organisation’s activities. Support functions are functions that support the execution of the primary functions and are similar for many organisations (e.g. financial accountancy, etc.).

The functions are reflected in the upper levels of the classification scheme and in Estonia the levels are named accordingly: funktsioon, allfunktsioon (function, sub-function). Classes and sub-classes (sarjad, allsarjad) derive from functions. It is important to bear this in mind when reading this chapter zero, since MoReq2 uses the blanket term class for all of these levels.

The classification scheme will serve as the basis for a list of record classes which must contain the names, classification codes and retention periods of functions and classes (see section 6.6) as well as information on whether and on what basis access to the records in the class can be restricted. The list can be supplemented with additional data necessary for records management. The list of record classes can be used to indicate whether and at which level of the classification scheme the ERMS implements the automatic inheritance of metadata and retention periods. For example, it is possible to determine that the marking of a function’s archival value or the data concerning the access restrictions of a class are inherited by default by all of its child classes, files and records. The classification scheme and list of record classes are used as the bases for the configuration of the ERMS.

The list of record classes is dynamic and is amended when necessary, e.g. when changes occur in the structure or duties of the organisation. If it is necessary to change the list of record classes or to send the classification scheme for approval, it is best to create an inquiry, a report or an extract in the ERMS, which can be saved in a format that can be processed and transferred electronically. This means further adjustment of reporting functionality described in MoReq2 section 3.4 Maintaining the Classification Scheme.

Additional information:

- Avaliku teabe seadus (Public Information Act)
- Regulation of the Government of the Republic “Arhiivieskiri” (Archival Rules)
- National Archives guidelines: http://www.ra.ee/et/noustamine-juhised/

### 6.3 Metadata for records and aggregations of records

With regard to the metadata of records, the source document currently in force in Estonia is “Dokumendihalluse metaandmete loend” (Records Management Metadata Set), the first
The implementation of MoReq2 in Estonia

version of which was issued by the Government Office in 2006. The original set was compiled on the basis of the standards EVS-ISO 15489-1 and EVS-ISO 23081-1 as well as foreign and international metadata models. The list differentiates between 13 metadata blocks:

1. metadata about mandates (regulatory requirements providing mandates for record creation);
2. metadata about functions (see section 6.2);
3. metadata about classification schemes;
4. metadata about classification units (class, sub-class, file);
5. metadata about records;
6. metadata about components (computer files);
7. metadata about access controls;
8. metadata about activities and transactions (e.g. registration of the record, opening of the file);
9. metadata about the organisation (description of the organisation that created the records);
10. metadata about groups/sections (e.g. department, division, working group);
11. metadata about positions/roles (e.g. manager, specialist);
12. metadata about agents;
13. address metadata.

The set contains 93 different elements and 60 element qualifiers, thereby providing a sufficient semantic base for the description of the most important data retained in ERMSs. The elements have been supplemented with references to equivalent elements found in foreign or international metadata models (including MoReq). The list is altered when required: when legislation is amended, new standards are adopted or a practical need for change arises. During the revision of the metadata set in 2012, the metadata elements used in the records exchange via DEC (see section 4.5) and for the disclosure of registers of records (see section 6.5) will be added together with new references to equivalent elements, and the textual part of the set will be updated.

The Records Management Metadata Set has been one of the source materials used for procuring and developing ERMSs in Estonia since 2006. The National Archives have used it as the basis for creating a list of metadata necessary for archiving and developing a universal archival module (UAM) (see section 6.6).

Additional information:


6.4 Creation and exchange of records
**Creation of records**

In accordance with the constitution, Estonia’s state institutions and local governments use Estonian as the language of public administration and everyone has the right to address these institutions in Estonian and receive answers in Estonian. Since the Estonian language includes many non-English characters, an ERMS implemented in Estonia must be capable of handling ISO 10646 standard compliant (Unicode) encoding. Also, the ERMS must have an Estonian language user interface (it is recommended that the user interface be available for adjustment to other languages).

The creation of records is based on the set of elements for the relevant record type, which is also used to develop the record templates used in ERMSs. The elements of records and the description of record types are discussed in the regulation of the Government of the Republic on the Common Principles of Administrative and Records Management Procedures. Among other things, the regulation provides for the confirmation of the set of elements for a record type through development of a data description. The elements of one record type – the letter – are established in the national standard EVS 882-1:2006, which has been planned to be revised in 2012.

The elements of a record type can partially coincide with the record metadata elements entered in the ERMS. In this case, the ERMS should be able to transfer the values from the draft record to the metadata or the other way around.

A certificate that meets the requirements set forth in the Digital Signatures Act is used when digitally signing records (see section 5.2). However, the signature is not an obligatory element for every record and may be absent if legislation does not require its presence in the case of the type of record at hand and if the record has been captured into the ERMS by an authenticated and authorised user and is permanently linked to or relatable to the necessary metadata. For example, a signature is not necessary in the case of informative letters (notices, etc.). If necessary, records will be confirmed with a digital stamp (see section 5.2).

It is advisable to create digital records with a long retention period (more than 10 years) in formats suitable for long term preservation (see section 6.6); this will be mandatory for public sector institutions as of 2013. This requirement should also be borne in mind in connection with the development and acquisition of ERMSs.

**Transition to the XML language**

After the establishment of the Document Exchange Centre in 2006 (DEC, see section 4.5), the transition to the XML language in the field of electronic records exchange was stipulated in the Government regulation on the Common Principles of Administrative and Records Management Procedures. At present, the first stage of the process has been completed and the requirement to use the XML language is met with regard to transferring record metadata (the record "envelope"); the implementation of the next stage is underway, with the XML language being gradually adopted for the purpose of creating records.

In the case of the creation of XML-format records exchanged through the DEC, it is necessary to use uniform data descriptions and take into account the guidelines issued by the Ministry of Economic Affairs and Communications on the development of XML data.
The implementation of MoReq2 in Estonia

descriptions of record types, the elements of records and metadata. The data descriptions are to be checked and approved by the Ministry of Economic Affairs and Communications, the National Archives and the Estonian Information System’s Authority, and published in the RIHA XML repository (see section 4.3). If the data description of a record type has been duly prepared and approved, the composition of elements of that record type is also thereby confirmed and must be followed in creating records of that type in any format.

The implementation of the XML format for records requires an ERMS to offer various functionalities: most importantly, support for the capturing, processing and displaying of records. An interface with an accounting system, personnel system or other information system may be necessary for the reuse of contents of an XML-record. There is not a finalised list of functionalities required from the ERMS for handling records in the XML format, since the needs of organisations are different and some functionality can be provided through other application software (e.g. the XML tool used for preparing legislation).

**Developing a data description of a record type**

The ability of an ERMS to “understand” (automatically process) the contents of a record and identifying information therein can only be used to reduce the amount of manual work in records management if the records are created according to the predefined and agreed structure. Record contents can only be processed in a uniform manner by all organisations if the structures of record types have been agreed upon at the national level. Estonia has chosen a path where record types will mainly be described using the bottom-up approach, i.e. on the initiative of institutions (or private sector companies), and in the XML format. The harmonisation of the descriptions and the creation of interoperability takes place through a central register (the RIHA XML repository, see section 4.3).

In 2010, the Government Office issued guidelines for compiling the XML data descriptions of record types, which will be revised in 2012 by the Ministry of Economic Affairs and Communications on the bases of user experience and suggestions. The guidelines describe the process of planning, creating and coordinating the development of data descriptions, and the annex of the guidelines lists the technical and semantic requirements for the XML schemes and documentation included in the data description.

The XML data description of a record type consists of both machine-readable and human-readable parts:

- list of the elements of the record;
- XML schema for the record type (XSD file);
- list of metadata that are specific to the record type (if necessary)\(^{16}\);
- XML schema of the metadata of the record type (if necessary);
- style sheets (XSL files);
- XML sample records of the record type;
- displays of the record type template and sample records.

\(^{16}\) The XML format container (record “envelope”) used in the DEC data exchange contains the metadata necessary for the automatic registration of any type of record upon arrival. As a result, the data description only has to be supplemented with the additional metadata that have to be transferred together with the particular type of record (if the attachment of additional metadata is required).
The implementation of MoReq2 in Estonia

In order to coordinate and publish XML data descriptions, the descriptions have to be entered into the RIHA XML repository. The Estonian public sector have adopted the XML-based e-invoice previously used only in the private sector, and implemented the XML format in the case of legislation (e.g. laws and regulations).

Additional information:

- *Eesti Vabariigi põhiseadus* (Constitution of the Republic of Estonia)
- *Keeleseadus* (Language Act)
- *Digitaalallkirja seadus* (Digital Signatures Act)
- Government Office’s guidelines for developing an XML data description of a record type: [https://riha.eesti.ee/riha/ Juhendid](https://riha.eesti.ee/riha/)
- XML repository: [https://riha.eesti.ee/riha/](https://riha.eesti.ee/riha/)

### 6.5 Registration and disclosure of records

**Registration**

Registration means linking a record with the records management system so that the record and its metadata in the register contain the same fully qualified classification code, which generally consists of the classifications codes of the parent function and class of the record and the record’s identifier in the register (e.g. 5-6/948 or 3.2-17/10-876023).

In Estonian records management tradition, registration is a separate obligation that is regulated by an organisation's records registration procedure. The main principles of the procedure are: (1) the single registration requirement, which was important in paper-based records management in large organisations and means that the organisations register their records centrally and structural units do not re-register the same records, and (2) registration based on the initiating record, which is especially used with regard to correspondence and means that each new initiating record (regardless of whether it is incoming or outgoing) is registered under its own number and the reply record is registered under the same number.
In such cases, an individualising number is added to the record’s fully qualified classification code in such cases (for example, 5-6/948-2 would be a reply record). The entire documentation related to a case may be registered under the same matter (case). Case-based systems always register all of the different types of records associated with a case under that particular case.

Registration applies to records in the sense of MoReq2, i.e. to so-called finalised or completed documents. Record drafts are not registered, except in cases where it is necessary to record the fact that they were forwarded or their state. The types of records and the composition of metadata that are to be registered have been established in a government regulation.

The serial numbers used in registers generally start over from zero at the beginning of each year.

**Register of records**

A register of records can have two meanings, one of which is used in everyday language and has developed historically while the other is primarily a legal term.

1) A register of records initially meant a book in which records were registered. The register book for incoming and outgoing letters was used to register the existence of a record by assigning a numerical identifier; in the case of correspondence, the registration was associated with the fact of receiving or sending out letters. The main goal of the register of records was to establish the existence of a record, preferably by using the record’s unique identifier, i.e. reference number, and thereby facilitate the timely performance of duties related to the record or monitoring validity periods. This goal is the same in the case of the second meaning of the register of records as established in the Public Information Act.

2) According to the Public Information Act, an organisation’s register of records is a digital database that is maintained by a state or local government agency or a legal person in public law in order to register records received by the organisation and prepared in the organisation and to ensure access thereto. Maintaining a register of records is mandatory for the aforementioned organisations. A register of records can be a completely independent database or a part of an ERMS.

The law establishes certain requirements for a register of records, the most important of which are the requirements to register (1) records that have been received and released, (2) legislation that has been prepared and signed and (3) contracts that have been entered into. The legislation also establishes the metadata to be fixed upon registration as well as the requirement that the register of records must be public to the extent prescribed by law. The public view of the register of records must be accessible through the organisation’s public website. The procedure for maintaining a register of records and the set of metadata to be fixed upon the registration of records are discussed in more detail in the regulation of the Government of the Republic on the Common Principles of Administrative and Records Management Procedures.

The legislation does not provide a description of the link between the register of records and one of the most important components of the ERMS – the classification scheme. In practice, the register and the classification scheme can be connected in two ways: (1) the registers
The implementation of MoReq2 in Estonia

are based on record types and the record type is determined upon registration with the register assigning a reference number to the record; (2) the registers are linked to a class or some other classification unit. The concept of the sub-register of records used in the Common Principles of Administrative and Records Management Procedures always means separate registers in practice and a register of records must be understood as a framework construction.

Disclosure

In Estonia, the disclosure of information is regulated by the Public Information Act. Information that has been recorded and documented upon performance of public duties is public information and if it is not subject to restrictions on access, access must be provided to it. Access to information is provided either by (1) disclosing the information or (2) complying with a request for information, i.e. releasing the information upon an oral or written request.

Information is disclosed through a public data communications network, meaning that institutions are obligated to maintain a website and disclose a certain amount of information on the website. The Public Information Act establishes the records and data that must be disclosed as well as the rules of disclosure for registers of records. The law is implemented in accordance with the guidelines of the Data Protection Inspectorate.

Since different software is generally used to handle an organisation’s ERMS and its website, it is necessary to interface the website management system and the ERMS for the purpose of disclosing the register of records. If the ERMS has a public online view, access to the view can be provided using a link on the organisation's website.

Although the data to be disclosed only makes up a part of the data in the ERMS, the disclosure of the register of records ensures that the record in question can be accessed in the original context, i.e. with links to related records.

The legislation stipulates which records must be (or can be) subject to restricted access and also establishes the record types access to which cannot be restricted. When disclosing information contained in a register of records, it has to be taken into account that records and metadata which cannot be accessed due to legal restrictions must not be disclosed before the period of access restriction has expired.

The legislation does not state whether the disclosure of the register of records has to be maintained for the entire retention period of the records and what should be done with the register data when the records have been transferred to the archives.

In the case of the disclosure of a register of records, it is necessary to:

- guarantee access to the metadata of the registered records;
- guarantee access to unrestricted digital records or provide the location references for records stored on paper or other media;

17 The Public Information Act is not applied in the case of classified information that is regulated by the State Secrets and Classified Information of Foreign States Act.
in the case of records with restricted access, display the metadata on the basis and data of the access restriction;

create an index and user manual in order to make it easier to find records and ensure that a full text search can be used to find data in the public view of the register of records, but not in the contents of the registered records, since the register also contains records with restricted access.

follow the good practice of web applications when publicly displaying the register of records online (the users should not have to repeat mouse clicks to reach the information they require, etc.).

Additional information:

- **Avaliku teabe seadus** (Public Information Act)
- **Isikuandmete kaitse seadus** (Personal Data Protection Act)

**6.6 Retention, disposition, transfer to the National Archives and destruction of records**

**Retention period**

All classes (see section 6.2) in an ERMS must be assigned a retention period. Retention periods are primarily established on the basis of the requirements set forth in legislation which, in certain circumstances, can also be obligatory for the private sector. If the retention period of the records of a class has not been provided in legislation, the retention period will be determined by the head of the organisation upon the approval of the list of record classes.

Although records in ERMSs are generally assigned the retention period of the appropriate class or file automatically (i.e. through inheritance), it must also be possible to set retention periods manually. Furthermore, an ERMS must allow users to determine events that trigger the calculation of the retention period or serve as the end points for retention periods. Retention period management is supported by the multi-level retention and disposition schedules described in MoReq2.

**Archival value**

In Estonia, public archives conduct appraisals to determine which records have archival value and will therefore be retained permanently. Records with archival value must be transferred to public archives and constitute a part of the national cultural heritage. An ERMS
must provide an option for marking the classes or files on which the public archives have rendered their appraisal decisions and identifying classes or files as having archival value or being subject to disposition and destruction pursuant to the usual procedure. For this purpose, the information concerning appraisal decisions is entered into the metadata of a class or a file. The ERMS must preclude the destruction of files or classes and the records belonging thereto if they have been identified as having archival value, regardless of the initial retention periods assigned to these files or classes.

Retention of digital records

There are two methods for retaining digital records and the distinction between the methods is mainly organisational. Firstly, retaining records in an ERMS, which may be the only place where records with short retention periods are stored, and secondly, the retention of digital records in an archive management system after their disposition from the ERMS. An archive management system can be a system maintained by an organisation, a service provider or public archives.

The ERMS may have other archival functionalities in addition to the functionality of managing retention periods. Estonian legislation does not provide requirements for digital archival software, although the OAIS (Open Archival Information System) model is usually followed in terms of architecture and functionality in accordance with the standard ISO 14721:2003 “Space data and information transfer systems. Open archival information system. Reference model”.

Retention of digital records in the National Archives

Records that have been created or received in the course of the performance of public duties and have been determined to possess archival value as a result of an appraisal are transferred to the National Archives (except when provided otherwise by law). According to the Archives Act that came into force in 2012, an organisation can transfer such records as soon as they are no longer necessary for the performance of its duties and has to transfer the records no later than 10 years after creating or receiving them.

In addition to records with archival value, public institutions can use the service of the National Archives to store digital records with no archival value if their retention period is longer than 10 years. The retention of digital records with shorter retention periods must be ensured by the institution’s own ERMS. Records must be transferred to the National Archives in accordance with the guidelines provided by the National Archives.

The National Archives has approved a list of formats that are suitable for the long term retention of digital records with archival value: XML (Extensible Markup Language); TXT; PDF (Portable Document Format), PDF/A format recommended; TIFF (Tagged Image File Format); PNG (Public Network Graphics); BWF (The Broadcast Wave Format); AIFF (Audio Interchange File Format); decompressed video; video formats created with the video compression method MPEG-2.

As of 1 January 2013, public sector institutions will be obligated to create digital records with long retention periods (in excess of 10 years) in formats that are suitable for long-term retention. This requirement ensures that records with a long retention period are created
The implementation of MoReq2 in Estonia

using file formats suitable for long term preservation and can be transferred to the National Archives securely and without additional processing.

**Transfer of digital records to the National Archives**

The architecture and functionality of a digital archive have been described on the website of the National Archives. The National Archives use the following method for receiving digital records:

![Figure 5: National Archives’ digital archives](image)

In order to facilitate the transfer of digital records with archival value to the archives, the National Archives have created a software tool: the Universal Archiving Module (UAM). UAM enables an archival scheme to be created using the classification scheme of an ERMS or its structure to be modified (as an example to merge classes). The records are exported from the ERMS to the UAM where they are (1) arranged and (2) described in accordance with the archival description rules. In the course of the arrangement, UAM enables the migration of records into file formats suitable for long term preservation (if necessary), etc. During the archival description phase, the archival description of the material is semi-automatically created based on the existing records management metadata.

In order to enable the use of the UAM, the ERMS must be capable of exporting data in the XML format; additionally, a mapping table in XSL format has to be created to transform the export into the XML format with semantics and structure supported by UAM. The UAM XML format is defined by an XML Schema (XSD) and available from the National Archives’ website.

If UAM has migrated computer files into archival file formats then both the original files and the files migrated into the file format suitable for long term preservation are transferred to the archives. The National Archives also accept records with digital signatures according to a similar procedure. Records can be transferred to the National Archives through the DEC (see
The implementation of MoReq2 in Estonia

section 4.5). As also stated in MoReq2, transferred records must not be destroyed in the ERMS before their successful transfer has been confirmed.

The UAM uses a web service to send both the archival description and the records to the archive storage through the National Archives’ ingest module. The archival description is linked to the archival information system (AIS), which is used to access records stored in the archives.

The basic digital archive solution is similar for organisations that need to retain records without an archival value for long periods.

**Destruction of records**

In the public sector, records cannot be destroyed before the National Archives have issued an appraisal report regarding the records. The destruction of records (as well as their disposition and transfer) must take place in a controlled manner and must be duly documented. A certain segment of metadata, or a metadata stub, is retained after the destruction of records. At the same time, an ERMS is responsible for ensuring the complete and irreversible deletion of the records and creating and retaining sufficient documentation on the destruction of the records.

**Additional information:**

- *Arhiiviseadus* (Archives Act)
- Regulation of the Government of the Republic "Arhiivieskin" (Archival Rules)
- Digital archival system and services: [http://www.ra.ee/et/digitaalarhiivindus/](http://www.ra.ee/et/digitaalarhiivindus/)
## APPENDIX 1: DIFFERENCES BETWEEN THE TEXTS OF MoReq2 (v1.04) IN ENGLISH AND ESTONIAN

The table describes the differences caused by mistakes in the original text (see section 2.3), as well as those caused by the distinct characteristics of the Estonian language.

<table>
<thead>
<tr>
<th>Ref №</th>
<th>MoReq2, v1.04</th>
<th>English version</th>
<th>Estonian version (translated into English)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>D01</td>
<td>Title page 2</td>
<td>This specification is available ...</td>
<td>The English language original of this specification is available ...</td>
<td></td>
</tr>
<tr>
<td>D02</td>
<td>Title page 2</td>
<td>Translations into selected languages are expected to be available at these sites.</td>
<td>Translations into selected languages are available at these sites.</td>
<td>By the time of publication of the translation, there are several translations available.</td>
</tr>
<tr>
<td>D03</td>
<td>Title page 2</td>
<td>It is also available in paper form ...</td>
<td>The English language original of this specification is also available in paper form ...</td>
<td></td>
</tr>
<tr>
<td>D04</td>
<td>Title page 2</td>
<td>--</td>
<td>(The title, the publisher and the copyright owner of the original) + Estonian translation by: © Riigikantselei, 2010 This translation has been validated by the DLM Forum</td>
<td>According to the licence agreement</td>
</tr>
<tr>
<td>D06</td>
<td>Section 1.3, last sentence</td>
<td>(see section 1.6 and appendix 3 for guidance on using and customising this specification)</td>
<td>(see section 1.9 and appendix 3 for guidance on using and customising this specification)</td>
<td>Correction of an obvious mistake confirmed by the MGB. Section 1.9: Customising this Specification, appendix 3: Use of this Specification in Electronic Form. Section 1.6: Intellectual Property Rights</td>
</tr>
<tr>
<td>D07</td>
<td>Section 1.8,</td>
<td>- - - this single specification cannot represent a requirement which precisely maps onto existing requirements without modification.</td>
<td>- - - this single specification cannot be a set of requirements which precisely maps onto existing requirements without modification.</td>
<td>Correction of an obvious mistake confirmed by the MGB.</td>
</tr>
<tr>
<td>Code</td>
<td>Section</td>
<td>Paragraph/Comment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D08</td>
<td>1.9, last paragraph</td>
<td>It has been prepared using Microsoft Word 2003 ...</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The English language original has been prepared using Microsoft Word 2003 ...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D09</td>
<td>2.1, 13.1: component</td>
<td>... the word “file” is avoided here to prevent confusion with the records management meaning of “file”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D10</td>
<td>2.1, 13.1: document</td>
<td>The word &quot;recorded&quot; in the definition does not imply the characteristics of a record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D11</td>
<td>2.1, 13.1: volume</td>
<td>A subdivision of a sub-file. Note: the subdivisions are created to improve manageability of the sub-file contents ...</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A subdivision of a file or sub-file. Note: the subdivisions are created to improve manageability of the file or sub-file contents ...</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Correction of an obvious mistake confirmed by the MGB. See also the previous comment, the introduction to section 3.3 (This section includes requirements relating to the use of volumes and sub-files, both of which are typically used to subdivide files which might otherwise be unmanageably large.), and requirement 3.3.3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D12</td>
<td>3.3, introduction, last paragraph</td>
<td>In summary: ... ♦ Each sub-file may contain one or many volumes; ♦ Volumes of different sub-files are created independently; ... ♦ Only one volume can be open in each sub-file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>In summary: ... ♦ Each file or sub-file may contain one or many volumes; ♦ Volumes of different files or sub-files are created independently; ... ♦ Only one volume can be open in each file or sub-file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Correction of an obvious mistake confirmed by the MGB. See also the previous comment, the introduction to section 3.3 (This section includes requirements relating to the use of volumes and sub-files, both of which are typically used to subdivide files which might otherwise be unmanageably large.), and requirement 3.3.3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D13</td>
<td>13.3, Volume, first sentences</td>
<td>Each sub-file can be divided into volumes ... In practice, most sub-files are not divided into volumes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each file or sub-file can be divided into volumes ... In practice, most files and sub-files are not divided into volumes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Correction of an obvious mistake confirmed by the MGB. See also the previous two comments and section 2.2 (Electronic File, Sub-file and Volume, para 4): Regardless of whether sub-files are used or not, files are sometimes divided “mechanically” into file...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D14</td>
<td>Section 2.2, Electronic File, Sub-file and Volume, first paragraph</td>
<td>This requirement is needed to prevent users employing text searches to investigate the contents of documents to which they are not allowed access.</td>
<td>Correction of an obvious mistake confirmed by the MGB. Elsewhere in section 2.2, it is stated that records are assigned to files. Moreover, it is already said that (2.2, Record and electronic record, para 2): - - - in MoReq2, the term record is used to refer to the informational content – the document(s) from which the record is made.</td>
<td></td>
</tr>
<tr>
<td>D15</td>
<td>4.1.22, note</td>
<td>This requirement is needed to prevent users employing text searches to investigate the contents of records to which they are not allowed access.</td>
<td>Correction of an obvious mistake confirmed by the MGB. The requirement states that the result list must not contain any record to which the user does not not have a permission to access. Moreover, it is already stated that (2.2, Record and electronic record, para 2): - - - in MoReq2, the term record is used to refer to the informational content – the document(s) from which the record is made.</td>
<td></td>
</tr>
<tr>
<td>D16</td>
<td>5.1.23, note 4, last paragraph</td>
<td>These situations can arise when a document has a record type permitting the application and inheritance of a disposal rule to that record from the record type rather than from the aggregation in which it is contained.</td>
<td>Correction of an obvious mistake confirmed by the MGB. See also the second half of the sentence: - - - inheritance of a disposal rule to that record - - -</td>
<td></td>
</tr>
<tr>
<td>D17</td>
<td>5.1.24</td>
<td>♦ transfer to an archive or another repository (see glossary).</td>
<td>Correction of an obvious mistake confirmed by the MGB.</td>
<td></td>
</tr>
<tr>
<td>D18</td>
<td>5.1.32</td>
<td>The ERMS must allow an administrative role to amend any retention and disposition schedule (apart from its unique identifier, see Requirement 5.1.6: maintaining an unalterable history of changes (audit trail),</td>
<td>Correction of an obvious mistake confirmed by the MGB.</td>
<td></td>
</tr>
<tr>
<td>D19</td>
<td>Chapter 8, introduction, second paragraph</td>
<td><strong>Presentation</strong> is producing a representation on-screen (&quot;displaying&quot;) or printing; it may also involve, as necessary, playing audio and/or video (see glossary).</td>
<td><strong>Presentation (see glossary)</strong> is producing a representation on-screen (&quot;displaying&quot;) or printing; it may also involve, as necessary, playing audio and/or video.</td>
<td>Correction of an obvious mistake confirmed by the MGB.</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>D20</td>
<td>9.2.4</td>
<td>… either as a date range (e.g. 24/12/2008 – 5/1/2008) or …</td>
<td>… either as a date range (e.g. 24/12/2008 – 5/1/2009) or …</td>
<td>Correction of an obvious mistake confirmed by the MGB.</td>
</tr>
<tr>
<td>D21</td>
<td>9.2.12</td>
<td>♦ the rate of retrieval of <strong>records</strong>.</td>
<td>♦ the rate of retrieval of <strong>documents</strong>.</td>
<td>Correction of an obvious mistake confirmed by the MGB.</td>
</tr>
<tr>
<td>D22</td>
<td>10.3.23, note</td>
<td><strong>For example, the time of creation and author of a document, also metadata identifiable from structured fields within documents if these exist, such as date and subject.</strong></td>
<td>–</td>
<td>Correction of an obvious mistake confirmed by the MGB.</td>
</tr>
<tr>
<td>D23</td>
<td>Section 10.7</td>
<td><strong>Electronic signature(s)</strong></td>
<td><strong>Digital signature(s)</strong></td>
<td>In Estonia, the signatures described in the section are known as digital signatures. The term “electronic signatures” is retained where appropriate (e.g. in the paragraph on the directive 1999/93/EC).</td>
</tr>
<tr>
<td>D24</td>
<td>Section 10.9</td>
<td>♦ <strong>Electronic watermarking</strong> (also referred to as <strong>digital watermarking</strong>), …</td>
<td>♦ <strong>Digital watermarking</strong> (also referred to as <strong>electronic watermarking</strong>), …</td>
<td>In Estonian, the terms “electronic watermark” and “electronic watermarking” are uncommon.</td>
</tr>
<tr>
<td>D25</td>
<td>10.13.6</td>
<td><strong>For at least one sub-category, the ERMS must support a hierarchy of at least five levels, from unrestricted access at the highest level to highly restricted access at the lowest level.</strong></td>
<td>For at least one sub-category, the ERMS must support a hierarchy of at least five levels, from unrestricted access at the highest level to highly restricted access at the lowest level.</td>
<td>A mistake confirmed by MGB. The original wording contradicts the test case for the requirement (see test case T10.13.2.2, description), as well as requirements 10.13.14–10.13.16, 10.13.22–10.13.23, 10.13.28, and test cases T10.13.3.3–T10.13.3.6, T10.13.6.1.</td>
</tr>
<tr>
<td>D26</td>
<td>10.13.12</td>
<td><strong>When a new hierarchical security</strong></td>
<td><strong>When a new hierarchical security</strong></td>
<td>Correction of an obvious mistake</td>
</tr>
<tr>
<td>D27</td>
<td>11.2.1</td>
<td>♦ &lt;100%&gt; of the anticipated total volume of documents managed by the system;</td>
<td>♦ &lt;100%&gt; of the anticipated total volume of records managed by the system;</td>
<td>Correction of an obvious mistake confirmed by the MGB. Other requirements in this section address records. Moreover, it is already stated that (2.2, Record and electronic record, para 2): - - - in MoReq2, the term record is used to refer to the informational content – the document(s) from which the record is made.</td>
</tr>
<tr>
<td>D28</td>
<td>11.2.3, note 1</td>
<td>This requirement, and that at 11.2.4, apply only to documents that can be presented in the form of pages. If the documents are unusually large, it may be necessary to extend the acceptable response time.</td>
<td>This requirement, and that at 11.2.4, apply only to records that can be presented in the form of pages. If the records are unusually large, it may be necessary to extend the acceptable response time.</td>
<td>Correction of an obvious mistake confirmed by the MGB. Requirements 11.2.3 and 11.2.4 are on retrieving and displaying records. Also, it is already stated that (2.2, Record and electronic record, para 2): - - - in MoReq2, the term record is used to refer to the informational content – the document(s) from which the record is made.</td>
</tr>
<tr>
<td>D29</td>
<td>Section 11.6, introduction, second paragraph</td>
<td>Organisations send their documents or records … to be indexed and stored by the ASP. The documents are then available for retrieval and presentation by the organisation’s staff …</td>
<td>Organisations send their documents or records … to be indexed and stored by the ASP. The documents/records are then available for retrieval and presentation by the organisation’s staff …</td>
<td>Correction of an obvious mistake confirmed by the MGB. If records are sent to the storage of ASP, the organisation must be able to retrieve them.</td>
</tr>
<tr>
<td>D30</td>
<td>Section 13.1: physical file, redaction, role,</td>
<td>… Source: PRO Functional Specification (see appendix 1).</td>
<td>… Source: Functional Requirements for ERMSs by the National Archives of the UK (see appendix 1).</td>
<td>Correction of an obvious mistake confirmed by the MGB. The name of the specification does not...</td>
</tr>
</tbody>
</table>
The implementation of MoReq2 in Estonia

<table>
<thead>
<tr>
<th>transfer, version</th>
<th>Further aspects of the correspondence between MoReq2 and ISO 23081 are in appendix 9.</th>
<th>Further aspects of the correspondence between MoReq2 and ISO 15836 are in appendix 9.</th>
<th>Correction of an obvious mistake confirmed by the MGB. The standard under discussion is ISO 15836 (the Dublin Core)</th>
</tr>
</thead>
<tbody>
<tr>
<td>D32</td>
<td>Appendix 5, last sentence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D33</td>
<td>Appendix 7, section 7.5, XML</td>
<td>In principle however, it can influence the format of record creation then the way in which the metadata is stored and expressed at capture and during later use; …</td>
<td>In principle however, it can influence the format of record creation, and the way in which the metadata is stored and expressed at capture and during later use; …</td>
</tr>
<tr>
<td>D34</td>
<td>Appendix 8, section 8.2, Relationship between Sections</td>
<td>(MoReq2) 10.15 Security Categories</td>
<td>(MoReq2) 10.13 Security Categories</td>
</tr>
</tbody>
</table>
# APPENDIX 2: FOOTNOTES IN THE ESTONIAN TRANSLATION OF MoReq2

<table>
<thead>
<tr>
<th>Ref №</th>
<th>MoReq2, v1.04</th>
<th>The text or content of the footnote (translated into English)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>FN 4</td>
<td>Section 1.3, fourth paragraph, first sentence</td>
<td>“Teavik” <em>(document)</em> – see glossary; “teavikuhaldus” <em>(document management)</em> – see section 10.3. (Translator’s remark)”</td>
<td></td>
</tr>
<tr>
<td>FN 5</td>
<td>Section 1.3, last sentence</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D06</td>
</tr>
<tr>
<td>FN 7</td>
<td>Section 1.9, List of formats</td>
<td>“The Estonian translation has been prepared using Microsoft Word 2003 and is published in the following formats: Microsoft Word 2003 (version 11), Adobe PDF (version 8), Open Office (version 3). (Translator’s remark)”</td>
<td></td>
</tr>
<tr>
<td>FN 8</td>
<td>Section 1.12, first paragraph</td>
<td>“In English, the level of mandation can be indicated with one verb only <em>(must or should)</em>, whereas in Estonian it is necessary to use different verbs or their forms, depending on the context. Thus, in the Estonian text the words “peavad”, “tuleb”, “ei tohi” also indicate that a requirement is mandatory, and the words “peaksid”, “tuleks”, “ei tohiks” also indicate that a requirement is desirable. (Translator’s remark).”</td>
<td></td>
</tr>
<tr>
<td>FN 9, FN 36</td>
<td>Sections 2.1 and 13.1, <em>juhtumitoimik</em> <em>(case file)</em></td>
<td>“In some environments, the term “asja toimik” is used in the meaning of “juhtumitoimik” <em>(case file)</em>. (Translator’s remark)”</td>
<td></td>
</tr>
<tr>
<td>FN 10, FN 37</td>
<td>Sections 2.1 and 13.1, <em>sari</em> <em>(class)</em>, note 1</td>
<td>“In the public sector of Estonia, it is recommended to use a classification scheme based on the functions of the agency, where the highest level is called “funktsioon” <em>(function)</em>. Thus, the MoReq2 term “sari” also corresponds to the terms “funktsioon” and “allfunktsioon” <em>(sub-function)</em>. (Translator’s remark)”</td>
<td></td>
</tr>
<tr>
<td>FN 11, FN 38</td>
<td>Sections 2.1 and 13.1, fail (component)</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D09</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>FN 12, FN 39</td>
<td>Sections 2.1 and 13.1, teavik (document)</td>
<td>“The term “teavik” (document) is not in commonly used and is introduced in MoReq2 to allow for better understanding of its content and requirements. The same term is also used as the Estonian equivalent for the term document in information sciences – see, for example, standard EVS-ISO 2789:2007 “Informatsioon ja dokumentatsioon. Rahvusvaheline raamatukogustatistika” (Information and documentation. International library statistics). In standard EVS-ISO 15489-1:2004, the Estonian equivalent for the term document – “dokument” – coincides with that for the term record (“dokument”). (Translator’s remark)”</td>
<td></td>
</tr>
<tr>
<td>FN 13, FN 40</td>
<td>Sections 2.1 and 13.1, teavik (document)</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D10</td>
</tr>
<tr>
<td>FN 14, FN 41</td>
<td>Sections 2.1 and 13.1, köide (volume)</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D11</td>
</tr>
<tr>
<td>FN 15</td>
<td>Section 2.2, Electronic File, Sub-file and Volume</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D14</td>
</tr>
<tr>
<td>FN 16</td>
<td>Section 2.2, Classification scheme, second paragraph, first sentence</td>
<td>“On virtual files see the explanation above – in &quot;Electronic File, Sub-file and Volume&quot;. (Translator’s remark)”</td>
<td></td>
</tr>
<tr>
<td>FN 17</td>
<td>Section 2.2, Class, first paragraph</td>
<td>“In the public sector of Estonia, it is recommended to use a classification scheme based on the functions of the agency, where the highest level is called “funktsioon” (function). Thus, the MoReq2 term &quot;sari&quot; also</td>
<td></td>
</tr>
</tbody>
</table>
### FN 18
Section 3.3, introduction, last paragraph
The footnote explains the difference between the texts in English and Estonian.
See D12

### FN 19
Requirement 3.4.5, note 1
“An example of forming a fully qualified classification code — see the introduction to Chapter 7. (Translator’s remark)”

### FN 20
Requirement 4.1.22, note 3
The footnote explains the difference between the texts in English and Estonian.
See D15

### FN 21
Requirement 5.1.19
““Triggersündmus” (trigger event) is a user’s or system’s action or another event which, if recorded, activates automatically a process or activity. (Translator’s remark)”

### FN 22
Requirement 5.1.23, note 4
The footnote explains the difference between the texts in English and Estonian.
See D16

### FN 23
Requirement 5.1.32
The footnote explains the difference between the texts in English and Estonian.
See D18

### FN 25
Chapter 6, Terminology, first paragraph, first sentence
“The statement is more appropriate in the English-language environment. In Estonian ICT, the equivalent for the word capture is often “hõivamine”. (Translator’s remark)”

### FN 27
Chapter 7, introduction, the paragraph explaining the construction of fully qualified classification code
“In the public sector of Estonia, it is recommended to use a classification scheme based on the functions of the agency, where the highest level is called “funktsioon” (function). (Translator’s remark)”

### FN 28
Requirement 9.2.4
The footnote explains the difference between the texts in English and Estonian.
See D20

### FN 29
Requirement
The footnote explains the difference between the texts in English and
See D21
<table>
<thead>
<tr>
<th>FN</th>
<th>Requirement/Section</th>
<th>Footnote</th>
<th>Page References</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Requirement 10.3.23</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D22</td>
</tr>
<tr>
<td>31</td>
<td>Section 10.7, Electronic Signatures</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D23</td>
</tr>
<tr>
<td>32</td>
<td>Requirement 10.13.6</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D25</td>
</tr>
<tr>
<td>33</td>
<td>Requirement 10.13.12</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D26</td>
</tr>
<tr>
<td>34</td>
<td>Requirement 11.2.1; requirement 11.2.3, note 1</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D27, D28</td>
</tr>
<tr>
<td>35</td>
<td>Section 11.6, second paragraph</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D29</td>
</tr>
<tr>
<td>42</td>
<td>Section 13.3, Volume, first sentence</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D13</td>
</tr>
<tr>
<td>43</td>
<td>Appendix 3, Requirement</td>
<td>“In English, the level of mandation can be indicated with one verb only (must or should), whereas in Estonian it is necessary to use different verbs or their forms, depending on the context. Thus, in the Estonian text the words “peavad”, “tuleb”, “ei tohi” also indicate that a requirement is mandatory, and the words “peaksid”, “tuleks”, “ei tohiks” also indicate that a requirement is desirable. (Translator’s remark).”</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>Appendix 3, penultimate sentence</td>
<td>“‘tõrge!’ (error) if the software is in Estonian. (Translator’s remark)”</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Appendix 3, Last sentence</td>
<td>“Näita ruudujooni” (Show Gridlines) if the software is in Estonian. (Translator’s remark)”</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Appendix 5,</td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D32</td>
</tr>
<tr>
<td>FN 47</td>
<td>Appendix 8, section 8.1, last paragraph</td>
<td>“The original version of MoReq is not translated into Estonian. (Translator’s note)”</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>FN 48</td>
<td>Appendix 8, section 8.2, <em>Relationship between Sections</em></td>
<td>The footnote explains the difference between the texts in English and Estonian.</td>
<td>See D34</td>
</tr>
</tbody>
</table>
APPENDIX 3: AMENDMENTS TO THE CHAPTER ZERO, 2012 (Version 2.0)

The table describes the amendments made in the course of the update (see section 2.5)

<table>
<thead>
<tr>
<th>Estonian chapter zero, v 2.0</th>
<th>Content of the change</th>
<th>Reason for the change</th>
</tr>
</thead>
<tbody>
<tr>
<td>The entire text</td>
<td>Linguistic corrections</td>
<td>Transfer of the function of records management coordination from the Government Office to the Ministry of Economic Affairs and Communications</td>
</tr>
<tr>
<td>Introduction, sections 2.5, 2.6, 3.1, 3.2 (Guidelines, good practice and best practice), 6.3, 6.4 (Transition to the XML language; Developing a data description of a record type)</td>
<td>Corrected or added – the parts of the text describing the coordination of records management development in Estonia, the developing process of the Estonian MoReq2 translation and chapter zero, and the issuing of Estonian records management guidelines</td>
<td>Section 2.5, 2.6, 3.1, 3.2 (Laws; Guidelines, good practice and best practice), 6.3, 6.4 (Retention of digital records in the National Archives)</td>
</tr>
<tr>
<td>Sections 3.1, 3.2 (Laws; Guidelines, good practice and best practice), 6.2, 6.6 (Retention of digital records in the National Archives)</td>
<td>Corrected or added – the parts of the text describing the organisation of archiving in Estonia and specifying the scope of the Archives Act, the issuing of the National Archives' guidelines, and the requirements of the new Archival Rules (classification scheme, formats suitable for archiving)</td>
<td>Entry into force of the new Archives Act and the new Archival Rules</td>
</tr>
<tr>
<td>Sections 3.2 (Ministerial regulations and directives; Standards), 6.4 (Creation of records), 4.4 (Additional Information), 5.3 (Additional Information)</td>
<td>The reference to the Dublin Core standard corrected (the Estonian version was updated in 2011); an example no longer relevant (reference to the Minister of the Interior regulation of 17.01.07, now repealed) removed; information about the revision of the “Letter” standard added; references to the X-Road guidelines and ISKE documents renewed</td>
<td>Revision or repeal of standards, legislative acts and guidelines</td>
</tr>
<tr>
<td>Sections 4.4, 4.5</td>
<td>Descriptions of the State Portal estei.ee and ADIT service renewed; information concerning the users of DEC updated; information about a new service “Create an e-invoice”</td>
<td>Development of existing services, new services</td>
</tr>
<tr>
<td>Sections 4.4, 5.1 (Digi-ID and Mobile-ID), 5.2 (Digital signatures; Encryption)</td>
<td>Information about authorisation used for X-Road data exchange added; the use cases of Digi-ID, descriptions of the electronic signature calculation and the BDOC-</td>
<td>Technical detailing</td>
</tr>
</tbody>
</table>
The implementation of MoReq2 in Estonia

| container revised; the description of the encryption and decryption of records specified |  |
Chapter “0“ – MoReq Governance Board Approval

Name Marko Lukičić
Title Translation & Ch”0“ Workgroup Leader
Signature
Date 8th August 2012

Name Aleksandra Mrdavšič
Title MGB Convenor
Signature
Date 9th August 2012