WORLD BANK GROUP

Right to Information

Managing Records and Information for Transparent, Accountable, and Inclusive Governance in the Digital Environment:

Lessons from Nordic Countries

Anne Thurston
International Records Management Trust

Right to Information

Managing Records and Information for Transparent, Accountable, and Inclusive Governance in the Digital Environment:

Lessons from Nordic Countries

Anne Thurston
International Records Management Trust

Victoria L. Lemieux
Series General Editor

Managing Records and Information for Transparent, Accountable, and Inclusive Governance in the Digital Era: Lessons from Nordic Countries

By Anne Thurston, International Records Management Trust

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
www.worldbank.org

Right to Information Series

The Right to Information Series brings forward current and ongoing research on issues related to transparency and the right to information. It aims to provide a range of information on policy, practice, experience, and frontier issues related to public sector openness and transparency, including the underlying functions and outcomes of open government efforts.

Project Leader and Right to Information Series General Editor:
Victoria Lemieux, vlemieux@worldbank.org

Working Papers Series Editor:
Stephanie E. Trapnell, strapnell@worldbank.org

Titles in the Right to Information Series

Right to Information: Case Studies on Implementation (2014),
edited by Stephanie E. Trapnell

Right to Information: Requests and Appeals Data in RTI Systems (2014),
by Jesse Worker with Carole Excell

Right to Information: Recent spread of RTI legislation (2014),
by Toby Mendel

Right to Information: Identifying Drivers of Effectiveness in Implementation (2014),
by Stephanie E. Trapnell and Victoria L. Lemieux

Designing Right to Information Laws for Effective Implementation (2015),
by Toby Mendel

Managing Records and Information for Transparent, Accountable and Inclusive Governance in the Digital Era (2015),
by Anne Thurston

Guide to the Implementation of Right to Information Laws (2015),
by Victoria L. Lemieux and Stephanie E. Trapnell

Contents

Acknowledgments

This study could not have been completed without the warm and generous support of officials in relevant agencies across the three countries studied—Estonia, Finland, and Norway. They agreed to be interviewed, patiently answered questions, provided valuable reference material, and reviewed drafts of the studies, correcting any misconceptions that they identified. Their open and honest assessment of challenges of providing high quality information in the digital environment has brought a fresh perspective to a key aspect of achieving transparency, accountability, and social inclusion that is often overlooked. Their assistance is deeply appreciated.

Overview

Introduction

This set of three case studies explores the intersection of openness, digital governance, and high quality information in Estonia,[1] Finland, and Norway with the aim of identifying lessons that will support the same objectives in lower resource countries. Openness, a key aspect of the international agenda for increasing transparency and accountability, for reducing public sector corruption, and for strengthening economic performance, rests on the principle that citizens have a right to know what their governments are doing and to benefit from using government information. Goals for open, accountable, and inclusive governance rest on the assumption that trustworthy information is available and can be shared meaningfully through strategies for digital governance. This assumption needs to be examined. Does reliable and complete information exist across lower resource countries? Can it be accessed readily? Will it survive through time?

The three Nordic countries are distinguished by and highly respected for their commitment to openness and social justice, low levels of corruption, and advanced use of technology to support economic development and high quality customer service provision. These countries also are distinguished by their recognition that high quality information is an essential resource for national development and that managing digital records and data effectively is an essential state function. Their experience offers valuable insights into the means of meeting international expectations for using information to support openness and economic growth. The case studies seek to answer four basic questions: What is involved in managing digital information? What are the benefits? What are the risks of not managing this resource? What are the challenges for the future?

Harmonizing Goals for Openness, Digital Governance, and High Quality Digital Information

Nordic societies share the political goal of encouraging strong social cohesion based on the core values of equal opportunities, social solidarity, and security for all. They emphasize social rights and the principle that everyone, including vulnerable groups in society, is entitled to equal access to services, particularly health and education, and to social justice. The three governments also share a strong focus on maximizing opportunities of digital government, with an emphasis on interoperability solutions for public administration and for sharing, coordinating, and reusing information to inform strategy-setting and long term planning. Poor quality information and difficulties in exchanging it between information systems limits their ability to use information resources effectively. In particular, Finland and Estonia share a strong commitment to using digital governance solutions to facilitate high quality services for citizens and to facilitate cross-border information flow.

All three countries support the importance of high quality public sector as the evidence base for policy and decision-making and cross-organizational services. They are able to demonstrate accountability and transparency by enabling citizens to access trustworthy records and data that demonstrate what the government has promised, what it has done, and how it has spent public funds. Each of the three countries has moved beyond simply managing technology to managing integrity and access.

The case studies explore the range of information management issues involved in achieving a reliable and sustainable evidence base of government information and using it effectively as a basis for openness and digital governance. Experience in the three countries highlights the requirement for effective legal and administrative control frameworks and for standards as the basis for achieving quality and integrity. The information management issues that these countries are addressing are generic, and the innovative solutions that they are developing have significant international implications.

Although the precise approach differs, all three countries invest in managing digital records and data as part of a whole, with the aim of harmonizing the way information is produced, shared, and used across government; supporting smarter governance; and increasing the efficiency and cost effectiveness of public services. The issues are common across the three countries, but each has particular lessons to share, and each faces challenges in its own context. The findings are complementary. Together, they form a coherent picture of a crucial global set of issues that must be addressed as a key aspect of supporting development in the digital environment.

High Quality Digital Information

ESTABLISHING QUALITY CONTROLS

Experience in the three countries demonstrates that building high quality evidence involves an interface between interconnected laws, standards, well-defined metadata architectures, and technology systems. All three countries practice lifecycle or continuum information management and apply clear standards in order to achieve consistent controls as a core aspect of digital governance. As the expectation of benefits from information systems grows, it has become increasingly important to link together public records, data, and the systems used to create and manage them. This means, for instance, that data entered directly into a database will need to be maintained according to standard requirements for protecting evidentiary value, for instance those governing appraisal, destruction, or transfer to secure long-term storage. This holistic approach, known as information governance, maintains the legal requirement to protect the integrity of records and data, while broadening the approach to managing information required as evidence, regardless of form or structure.

All three countries apply guidelines and mandatory requirements as the means of achieving high quality information and ensuring that digital records can be shared across systems. Interoperability initiatives within and between governments require the ability to exchange information effectively, and this in turn requires standardized information structures. By specifying clear requirements for creating and structuring records generated by digital systems, the governments are able to produce reliable records as evidence of policies, actions, transactions, expenditure, precedents, and rights, and to use them as a basis for openness.

Metadata capture through registration systems, the traditional basis for maintaining control of public sector information in many European countries, remains central to digital records and information management strategies. Metadata registration makes it possible to link the content and context of the records, to describe them in a meaningful way, and to manage them securely. It provides the foundation for building information integrity and legal authority in the public sector, because once a record is registered and its context is fixed, it is difficult to alter it or delete it without authority. Metadata documents how the records were created, managed, and used and their relationship to other records. Any subsequent changes and anything that happens to the record also are doumented through metadata, thus providing an audit trail of context and changes in status that makes it possible to identify fraud or illegal actions.

The records and information management standards in use in the three countries include data models, as well as requirements for records structure and metadata, and for functionality in Electronic Records Management Systems. They describe arrangements for registration, filing, and retention, and they define XML-scheme for exporting records from records systems to secure long-term storage. Norway and Finland have developed their own standards, while Estonia uses MoReq®, a specification of modular requirements for digital records systems developed by the DLM Forum, a European wide organization of national archives, enterprises, and research organizations with an interest in digital records management

BENEFITS OF DIGITAL RECORDS MANAGEMENT

The benefits of effective digital records management are illustrated in the case studies and summarized here.

- The public can have confidence in the credibility, authenticity, and integrity of the information, and public sector agencies can use them effectively for planning and monitoring programs, activities, and expenditure.
- It is possible to rapidly trace, relate, and compare policies, decisions, actions, and expenditure accurately over long periods of time as a basis for an informed and socially just society.
- Accountability and transparency are safeguarded. An audit trail of any changes or unauthorised use of the records makes it possible to detect and trace corruption.
- Records can be opened to the public systematically and privacy rights can be protected. Any restriction on opening records can be justified and documented.
- Right to Information requests can be met rapidly and reliably. Documents can be tagged when there is a legal restriction on publication.
- Records can be migrated to new formats and software and hardware environments as necessary.
- Standardized interoperability rules can be applied effectively, making it possible to interface dispersed information systems, such as document management systems, accounting systems, or information systems specific to an organization's activities, and to reuse information.
- Records can be securely and systematically extracted from diverse digital systems and transferred to long-term digital custody, where they can continue to meet meet legal, administrative, fiscal, or other evidentiary needs through time.
- Information loss is minimized. The high risk of holding digital records outside secure managed storage decreases.

IMPLICATIONS FOR DATA MANAGEMENT

The same issues apply to data management. There is growing awareness of the value of data for improving policy decisions and service provision, as well as for research, planning, and monitoring, and for public use, and there is recognition that data should be better managed and used. Open data is seen as a key aspect of information management/information governance strategies. Achieving better quality data and more effective use of data involves the same management principles that apply to records and a clear understanding of the relationship between these two forms of information. Where public sector data has not been protected and preserved systematically, it often has been lost inadvertently and cannot be exchanged and reused effectively.

As is the case with records, the ability to understand, use, and preserve databases requires continuous use of standardized metadata to document the origin and use or the database and the way it has been managed. Data models, processing rules, and guidelines for standardized structures and mandatory metadata fields are being defined in standards. Control mechanisms are being strengthened to provide quality, enable traceability, protect privacy, and support

access through time. These include clearly defined interfaces for converting datasets from relational tables to XML files, making it possible to bring records contained in databases to secure long-term storage.

Key Issues for the Future

The case studies describe challenges the three countries have identified for managing records and information in relation to rapidly escalating technological change and citizens' growing expectations for access. All three countries are addressing all of these challenges, but each has its own approach in relation to its history and national commitments. Estonia is building the regulatory framework and system functionality needed to create seamless data exchanges across functions, while simultaneously addressing legacy issues arising from the rapid transition to digital governance. Finland is redefining laws, regulations, roles, and responsibilities for managing records and data in relation to the intersecting requirements for digital governance, access to information, and records and data management. Norway is in the process of defining simpler, cheaper automated means of extracting records and metadata from records systems to enable greater benefits for society.

These challenges are inevitably the same for all countries aspiring to use digital records and data effectively to support openness and economic growth. The longstanding role of the national archives, as the agency with statutory responsibility for managing and protecting the evidentiary value of records, is ongoing. However, the laws, administrative placement, and responsibilities for information management must now be reconsidered, broadened, and extended to support a coordinated approach to goals for openness and digital governance, including access rights. Logical coherence in metadata structures across record generating systems, advanced search functionality based upon defined criteria, and easy to master user interfaces will offer enormous advantages for future ability to strengthen transparency and accountability, anti-corruption strategies, citizen engagement, and economic development. Countries that do not develop requirements for managing digital records will be at a significant disadvantage in the digital environment.

Less well-resourced countries, where these principles may not yet be applied, have an opportunity to consider the value of the essons learned in the Nordic countries in relation to their own development goals. They may wish to begin by carrying out a simple risk analysis to determine whether relevant laws are in place and have been harmonized, and whether clear manadatory requirements have been developed and implemented for creating, structuring, using, and preserving trustworthy records generated by digital systems. The answers to these questions will be help to determine whether trustworthy digital information is available to meet international development goals for open, accountable, and inclusive governance or whether a deeper approach is needed to move beyond simply managing technology to managing integrity and access.

Note

1. Estonia may be known as a Baltic or as a Nordic country. In this study it is referred to as a Nordic country because of the goals and strategies that it shares with countries in the Nordic region.

Information Governance and the Information Society
Estonia

Introduction

Estonia is distinguished by its cutting edge use of technology to support economic and social development and its parallel commitment to managing digital information as the evidence base for an effective modern public sector and high quality service delivery. Its innovative strategies for sharing information across government and making it available to citizens and the private sector illustrate the benefits of an integrated approach to digital governance, openness, and information management.

A small country in Northern Europe, Estonia is strategically positioned as the gateway between Europe and Russia; for centuries it experienced wave after wave of occupiers. Annexation by the Soviet Union in 1940, disrupted briefly by German occupation, lasted until 1991 and resulted in large-scale deportation, execution, or immigration of Estonians. Through these experiences, Estonia developed an orderly, highly adaptable culture that is deeply committed to freedom, self-determination, and preservation of national identity. Within a short time of reaching independence, the nation committed itself to using technology to support democracy, services to citizens, and sustainable economic growth.

In 1991 Estonia had very little IT infrastructure and few resources for large scale IT development, but from the mid 1990s onward, its IT infrastructure and skill base developed rapidly. The Government invested in centralized development of core components and support systems to keep costs low, and this resulted in highly innovative and efficient solutions. After Estonia joined the European Union in 2004, and was eligible for technical support, it was able to increase the pace of its rapid advance. The values of innovation, openness, and transparency, deeply rooted in Estonian administrative culture, are expressed in Estonia's concept that public sector information should be available to the public without the public having to ask for it.

The initial focus on information technology has broadened to incorporate a growing emphasis on high quality digital information as an integral component of the ICT management environment. Estonia's approach to managing the quality and accessibility of information is to apply the internationally agreed records management principles of authenticity and integrity to any type of public sector information that can serve as evidence, whether it is paper based, a relational database, or system generated digital records.

Estonia joined the Open Government Partnership in the spring of 2012. Its main goals in joining were to draw attention to the quality of state governance and learn from the experience of other states, while sharing its own good practices, especially in the areas of e-governance and public sector ICT use.

Digital Governance Environment

Interoperability and an emphasis on free and open use of the Internet are cornerstones of Estonia's technology development. Interoperability rules were introduced at the end of the 1990s, before most government systems were established, and today most public databases are interoperable. European Union investment, including training, has had a major impact on IT development, and if the EU were to cease funding development, the rapid progress to date could be difficult to sustain. However, the achievements are not simply a result of funding. Even after European Union investment in technological development began, the government continued to emphasize centralized core systems and principles across the public sector. This has helped to keep ICT expenditure lower than in other European countries and to produce effective results.

Estonian citizens have benefitted significantly from technological developments. For over a decade, they have been using on-line services for banking and for communicating with the state, which is now virtually paper-free in many areas of public administration. All core information services for citizens are available on the web. For instance, 98% of Estonians use online tax declaration; any doctor, with a patient's consent, can consult a medical history, and it is possible to establish a business rapidly and deliver all reports electronically. Estonia has an e-tax board, e-police, e-school, e-health, e-business, and an e-voting system. Information systems are aimed increasingly at users and services and at linking the whole Estonian information system into a common logical unit comprising public records, data, and the systems used to create and manage them.

As Estonia has moved rapidly toward digital governance, it has become increasingly clear that a high level of service provision must be underpinned by well-developed structures for managing the integrity and preservation of system generated records and data, and for accessing and preserving them through time. Linking information management to efficient, quality service provision is increasingly seen as a key aspect of developing fully electronic processes, improving reporting, increasing transparency, and protecting the evidentiary value of records on any media for as long as they are required.

While there is a long way to go in terms of widespread awareness raising and developing practical tools and guidelines, the importance of managing information for the transition to

the information society is spreading. Given that most public records in Estonia are created, exchanged, and received electronically, the Government works to ensure that digital information can be shared securely and efficiently. Once information has been gathered from citizens, agencies across government are able to reuse it. At present, records management and archival management are administered separately but collaboratively. However, there is a growing awareness that they are part of a whole.

Legal Framework

CONSTITUTION[1]

The Estonian Constitution guarantees all citizens free access to public information by making all government agencies and local authorities and their officials legally responsible for providing information about their activities to any citizen of Estonia. The only exceptions are where the law prohibits disclosure or where the information is intended exclusively for internal use.

PUBLIC INFORMATION ACT[2]

Estonia's Public Information Act was passed in 2000 to underpin democracy, the social rule of law, and an open society. It ensures that all citizens are able to access public information in order to exercise their rights and freedoms, meet their obligations, and monitor the performance of public duties. The Act creates a presumption of openness unless there is a reason for legal closure, for instance in relation to personal privacy. It requires information holders to ensure access to the information in the quickest and easiest manner possible. Access must be granted without charge unless the law prescribes payment for direct expenses relating to the release of the information.

ARCHIVES ACT[3]

The Archives Act, which was passed in 2011, defines a record as information on any medium created or received in the course of the activities of an agency or person; it defines an archival record as one that has been determined, through appraisal, to contain evidence of facts or activities of long term value to the nation. The Act requires that agencies and persons performing public duties ensure the preservation and usability of archival records by transferring them to the National Archives when the records are no longer needed for the performance of their duties, or within 10 years of their creation or receipt. The Act addresses the appraisal, acquisition, organization, and preservation of archival records, and it mandates that access to them must be unrestricted unless legal restrictions apply, for instance under the Public Information Act, the Personal Data Protection Act, or the the State Secrets and Classified Information of Foreign States Act.

Administrative Framework

MINISTRY OF ECONOMIC AFFAIRS AND COMMUNICATIONS[4]

The Ministry is responsible for secure technological development and innovation policy, as well as for establishing a user-friendly service environment. It drafts and implements economic policy and evaluates its outcomes, providing high-level coordination of information technology and interoperability issues, and taking political actions where necessary. The Ministry is a member of the DLM Forum, a community of public archives and interested parties from government, commercial, academic sectors that are interested in information governance. Founded by the European Commission in 1996, the Forum is a not-for-profit foundation providing industry specifications and serving members from across Europe and the rest of the world.[5]

Two key structural divisions of the Ministry, the Department of State Information Systems and the Department of Information Society Services Development, play an essential role in information governance. The Information System Authority,[6] a separate agency that reports to the Ministry, develops and has day-to-day oversight of a range of interconnected information systems.

Department of State Information Systems[7]

The Department is responsible for coordinating the development and administration of the national information system through the Information System Authority, with the aim of providing the best possible services to citizens. This includes providing the basic infrastructure for connecting important state information systems and their data; advising public service providers on managing their information systems; implementing policies for maintaining the core IT infrastructure, including interoperability and open data regulations; coordinating state IT-policy and development plans for state administrative information systems; developing and implementing IT-related legislation; managing government IT projects, budgets, and procurement; and overseeing IT standardization.

Information System Authority

The Authority is in charge of implementing requirements developed by the Ministry, including oversight of a range of a range of interconnected systems:

- **Administration System of the State Information System.**[8] This overarching information system provides information on the state's information systems and databases, the data collected and processed in the various information systems, the services provided, and who is using them.
- **Data Exchange Layer X-Road.**[9] This is a platform-independent secure central infrastructure that enables trustworthy communication between public sector information systems. Launched in 2001 to support the Public Information Act, the X-Road enables secure and cost effective Internet-based data exchange between databases belonging to the state information system. It allows public institutions, private sector enterprises, and citizens to securely access and exchange data to facilitate service provision. It connects over 1000 institutions

and several hundred information systems, and it facilitates several thousand machine-to-machine and web services.

- **Public Key Infrastructure.**[10] The infrastructure enables secure digital authentication and signing. It supports solutions for establishing electronic identity and forwarding data using an encryption key pair: a public encryption key and a private decryption key. While the state undertakes to assure the existence and functioning of a public key infrastructure, a large part of the serice is purchased from the private sector, for instance, certification and the infrastructure for distributing the public key.
- **Document Exchange Centre.**[11] This is a secure, virus and spam free infrastructure for transmitting documents (for instance, letters, draft legislation, financial documents, electronic forms) together with metadata, using the secure data exchange layer X-Road. It makes it possible to interface dispersed information systems, including, for instance, document management systems, accounting systems, or information systems specific to an organization's main activities. The DEC also supports the transfer of documents to appropriate long-term repositories. It is based on the entity model described in ISO 23081-2 Records Management Processes.[12] Citizens and entrepreneurs can use the state portal[13] service, Minu postkast (My Mailbox), to send and receive letters to and from any state or local government agency that uses DEC.[14] Smaller agencies that process their documents mainly in a document management system often provide electronic forms that citizens can complete and submit via Minu postkast. In the future, the forms will be pre-filled with the data already existing in the state information system, and citizens or entrepreneurs can monitor the progress of an application process.

Department of Information Society Services Development[15]

The Department is in charge of policies for effective information society services, records management, and information governance. It links digital records management to service provision to support electronic handling and procedural processes, improve reporting, increase transparency, and safeguard and preserve information on any media as evidence. The aim is to increase citizens' and officials' awareness of and satisfaction with state digital services, strengthen the potential for the information society, and enhance the efficiency of state policy formulation through high-quality information and data usage.

The Department has issued a series of guidelines, for records managers in state and local government agencies and for service providers, to support user-friendly and efficient information services.[16] These guidelines are being translated into English. In December 2014, the Department published 'Guidelines on Minimum Requirements for Estonian Public Sector Document and Records Management Systems' to enable agencies to describe, evaluate, and compare the strength of document and records management systems within the state information system. The aim is to improve management and administration processes, enhance the interoperability of records management systems, and facilitate document and data exchange.[17] The Guidelines support the provisions of the Archives Act and the Public Information Act for ensuring the preservation and usability of records. They rest on international records and information management good practice standards[18] that define requirements for managing digital

records. In addition, the Department of Information Society Services Development and the National Archives have jointly prepared a standardized set of minimum metadata requirements based on an extensive study of metadata requirements in countries including the UK, Germany, Canada, and Norway.[19]

Estonia has achieved significant progress in managing its records and information. Functional classification schemes have been designed, and retention periods defined. Electronic registers are maintained across government agencies and are available on agency websites, enabling citizens to find and read the records they need. Access restrictions on records are described explicitly, and the registers include descriptions of sensitive records closed for legal reasons so that citizens will know that they exist and can make enquiries about them.

The guidelines and metadata requirements, which are used increasingly for structuring and describing records, are beginning to make a fundamental contribution to national goals for digital governance. They help ensure that records held in records management systems are trustworthy and easy to find and that they remain reliable over long periods. They make it possible to use records as evidence of facts or activities by documenting their content as well as their context in terms their creation, management, use, and relationship to other records. The standardized metadata greatly enhance the ability to search across public document registers, to exchange records between organizations and information systems via DEC, and to archive and reuse information.

A Records Management Board has been established to determine the main directions of digital records management development, review and discuss legal issues, and to develop guidelines to regulate records management and support their implementation. Ultimately, the aspiration is to manage the information lifecycle/ continuum as a whole under one ministry, with a common approach and common rules. The Board includes the records management officers of all ministries, along with representatives of local governments, the National Archives, and the Ministry of Economic Affairs and Communications.

NATIONAL ARCHIVES[20]

Since 2012 the National Archives has been a subordinate agency of the Ministry of Education and Science. Its main tasks are to ensure the preservation and usability of society's written memory for future generations, and to provide access in order to facilitate comparative research and an historical context for development. The Archives collaborates directly with many ministries, most importantly with the Ministry of Economic Affairs and Communication, on issues relating to the information society. The Archives, which has extensive experience in digital information management, supports the appraisal, extraction, transfer, ingest, and preservation of digital information to the Archives repository.

Records management is not within in the scope of the Archives Act, but the Archives has contributed to guidelines, principles, and standards for digital records management issued by the Ministry of Economic Affairs and Communication as part of the national legal framework. The Archives works to ensure that everything that can be opened is open, that government agencies are supported in protecting information integrity, and that records and data in any format that have long-term evidentiary value are transferred to the Archives.

All Estonian public archives are part of a common information system, with common access tools and a common digital repository service. The Archives has developed excellent access to

its holdings. It maintains over 20 databases of archival descriptions that facilitate easy access to state archives, including paper and digitized records, film archives, maps, audio recordings, moving images, photos, and genealogic materials.[21] Digitized records form the bulk of this material, but the volume of born digital holdings is growing. The databases provide access to approximately 7.8 million description units, organized according to international professional principles and accessible through keyword searches. There is no charge for access to records preserved in the National Archives, and access is unrestricted unless there are specific restrictions established by law.

The Archives stays at the leading edge of professional development through its ongoing involvement with international and European professional programs. The E-ARK research project,[22] funded by the European Commission ICT Policy Support Programme, is particularly significant. In co-operation with commercial systems providers, research institutions, and other European national archives, the project is developing a scalable pan-European methodology for reducing risk of information loss by synthesizing existing national and international good practices for keeping records and databases authentic and usable through time. The Archives also participates in APEx, a Europe network of excellence that supports the Archives Portal Europe and includes information from nearly 900 European archival institutions.[22] The National Library of Estonia participates in the EU funded 'Collaboration to Clarify the Costs of Curation (4C)' project,[24] a Pan European Initiative that addresses the issues of risk, quality, and sustainability in digital; the National Archives intends to use the outcomes.

The Move to Information Governance

In 2013, a Ministry of Economic Affairs and Communications' Green Paper on the organization of public service delivery described the need to move from records management to a more holistic approach to information governance. Implementing this concept is part of the Government's Digital Agenda 2020.[25] The aim is to support smarter governance and help increase the efficiency and cost effectiveness of public services. An analysis of current developments and experiences in records management and information governance has been completed, and a changeover strategy is being prepared to plan the necessary measures, activities, and priorities.[26] This will not change the essential importance of managing records as evidence, but it will involve a broader approach to managing information across government, regardless of its form or structure, according to internationally agreed information governance principles. This will mean, for instance, that data entered directly into a database will need to be maintained according to standard requirements, for instance those governing appraisal, destruction, or transfer for long-term storage to a digital repository.

Open data is an essential part of the growing emphasis on information governance, and the Ministry of Economic Affairs and Communications has made it a key focus area. The view is that the government has an abundance of data created through its information systems, but the data could be better used to improve poicy decisions and service provisions. The aim is to significantly increase public sector capacity to apply data analytics solutions and make high quantity, precise, trustworthy data available to the public as well as to the private sector as a basis for developing new services or products. The precise means of relating open data to information governance is being defined.

National collaboration on open data is managed through a cross-government board led by the Ministry. The Board is working on priorities on defining the new laws, procedures, and structures that will be needed to govern data collection, management, and public release. There are issues to be resolved in terms of developing the open data portal, and as yet there are few practical arrangements in place. Half a dozen institutions have published data to the portal, including the Ministry of Finance, which has released budget data, and the statistics Office. The National Archives, which is represented on the Board, is one of the first large-scale open data providers, having released all of the archive description databases.[27] The aim is to open all public registers as live data during 2015, although it is not yet be possible to make new metadata available daily as is done in Norway. Although the aim is to open all public data as rapidly as possible, the Data Protection Agency and the Ministry of Justice have started to analyse potential threats to individuals' rights and state security if all data were to be published as open data. The study will help to define the pace at which data is opened.

The transition from records management to information governance is at an early stage, and there are still more questions than answers. For the transition to succeed, it will be essential that all relevant parties, including top management, IT personnel, and information managers, understand the significance of the change and their role in supporting it. The maturity of records management and information governance is variable from agency to agency, and success will require ongoing state of the art research, widespread dissemination of guidelines, and training. It is likely that it will be several years before information governance principles are implemented practically throughout the Estonian public sector.

Several Information governance initiatives are already underway. For example, the Ministry of Economic Affairs and Communication has analyzed some of the best-used public services in relation to information governance and, based on the results, it has prepared guidelines for managing and evaluating information quality in relationship to public sector e-services. In parallel, the National Archives has started to create practical guidelines for classifying and appraising information held in relational database systems to support agencies in extending their records retention plans beyond traditional systems.

Challenges

When European Union funding made it possible to kick start extensive work on ICT innovations at the beginning of the century, new systems were introduced as funds became available. Many aspects of long-term information management and of semantic and technical interoperability tended to be neglected. Now as the IT systems are more than a decade old, legacy issues are beginning to be visible. In the same way that information systems often were not properly documented initially, the functionality needed to support information retention, destruction, and export for transfer to long-term repositories often was left out of the equation, with long term consequences.

As an example, the security algorithms in the digital signature format set up in the early 2000s to keep signatures secure are becoming obsolete, making digitally signed records potentially vulnerable to hacking. A new format was introduced in January 2015 to add higher security

levels, but now many agencies now must address the legacy problem of what to do with information signed digitally over the last 15 years and still held in live agency systems. Had retention and disposition rules been in implemented, these digitally signed records could have been systematically destroyed when they ceased to have value or transferred to the National Archives where they could have been decrypted. A re-signing mechanism is being developed to ensure the authenticity of records through time, but it will be costly to implement. In the meantime, the content of the records will be accessible, but the older algorithms may not be available to validate the signatures, which will undermine the authenticity of the records. The challenge for the future will be to develop longetivity principles for government systems that allow taking up new standards and formats as they emerge without major costs, including the timely destruction and transfer of legacy records.

A related issue involves the lack of standardized metadata requirements in the early records management systems. At the time that many of the systems were set up, ad hoc metadata structures and data models were developed. This has made the uptake of standardized interoperability rules more challenging and time consuming than it would have been had metadata requirements been standardized early on. It also has undermined the ability to mange the lifecycle/ continuum of the records systmatically. However, in general, the public sector has acknowledged the need for standardized rules, and the situation is gradually improving as metadata rules are now commonplace when systems are replaced or updated.

The lack of explicit rules on the quality and extent of record descriptions also presents a challenge. While the public sector now generally accepts the requirements for publishing descriptions of records on their websites, agencies sometimes use generic titles and descriptions to divert attention from the records' content. Where this happens, users find it difficult to track an issue through the agency registers. This has an impact on the agencies' ability to open records and data proactively. Also, agencies sometimes try to set unjustified restrictions on data to avoid publishing it openly. This has an impact on the reuse and research value of the information. However, the Estonian Data Protection Agency is constantly working on this issue, and the situation is gradually improving as public sector institutions employ new staff members who have grown up in the networked environment and recognize the importance of establishing data quality.

As a final example, the interoperability of structured data information systems (public databases) has led to a situation where an agency maintaining a database is not necessarily the information creator, because when databases are connected to the X-Road, virtually any other agency can use the data and mash it up into new services. As new data is added there are difficulties in reflecting the provenance and distributed context of the data, which in turn has consequences for classification and appraisal. Work on this issue is at an early stage, but it will need to be solved before information governance can become a reality.

Conclusion

Estonia is making one of the most rapid transitions to an information society of any country in the world, and Estonians are experiencing substantial benefits. However, like other technologically advanced countries, the Government of Estonia is starting to experience challenges in managing the authenticity and integrity of its digital information. It is in the process of studying and applying internationally agreed standards and is drawing on experiences from other countries that also are defining new solutions for managing records and data as a national resource. As Estonia moves toward enhanced interoperability, security, and digital continuity through greater standardization, enhanced information governance is making an increasingly important contribution to achieving openness, transparency, and self-determination. Other countries, whether they are wealthy or less well resourced, will have much to learn from Estonia's bold and creative approach to the issues involved.

Appendix A. List of Key Records Management Standards Used in Estonia

Estonian records professionals have studied international records management standards carefully and used them as the basis for moving forward quickly and effectively in managing digital records.

- Information and Documentation. Records Management. Part 1: General (EVS-ISO 15489-1:2004)
- Information and Documentation. Records Management. Part 2: Guidelines (EVS-ISO 15489-2:2004)
- Information and Documentation. Records Management Processes. Metadata for Records. Part 1: Principles (EVS-ISO 23081-1:2006)
- Information and Documentation. Records Management Processes. Metadata for Records. Part 2: Conceptual and Implementation issues (EVS-ISO 23081-2:2011)
- Information and Documentation. Work Processes Analysis for Records (ISO/TR 26122:2008)
- Information and Documentation. The Dublin Core Metadata Element Set (EVS-ISO 15836:2011)
- Information and Documentation. Vocabulary (EVS-ISO 5127:2004)
- Requirements of Information Technology in Estonian Language and Cultural Environment (EVS 8:2008)

- Information and Documentation. Elements of Records and Requirements for Record's Layout. Part 1: Letter (EVS 882-1:2013)
- Information and Documentation. Principles and Functional Requirements for Records in Electronic Office Environments. Part 1: Overview and Positions (EVS-ISO 16175-1:2013)
- Information and Documentation. Principles and Functional Requirements for Records in Electronic Office Environments. Part 3: Guidelines and Functional Requirements for Record in Business Systems (EVS-ISO 16175-3:2012)
- Modular Requirements for Records Systems (MoReq2010)

Notes

1. Constitution: https://www.riigiteataja.ee/en/eli/530102013003.
2. Public Information Act: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/510072014004.
3. Archives Act: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/526092014003.
4. https://www.mkm.ee/en.
5. http://www.dlmforum.eu.
6. https://www.ria.ee/en/.
7. http://riso.ee/en.
8. https://www.ria.ee/administration-system-of-the-state-information-system/.
9. https://www.ria.ee/x-road/.
10. https://www.ria.ee/en/?id=27307.
11. https://www.ria.ee/dec/.
12. http://www.iso.org/iso/catalogue_detail.htm?csnumber=43390.
13. www.eesti.ee.
14. In February 2015, 660 agencies were using the DEC.
15. https://www.mkm.ee/en/objectives-activities/information-society/information-society-services
16. https://www.mkm.ee/en/objectives-activities/information-society/information-society-services;
16. https://www.mkm.ee/en/objectives-activities/information-society/records-management-information-governance.
17. The guidelines draw on international standards listed in Appendix A, particularly the Modular Requirements for Records Systems (MoReq2), ISO 16175-1:2010 Information and Documentation—Principles and Functional Requirements for Records in Electronic Office Environment; ISO 23081-2 Metadata for records. Part 2: Conceptual and Implementation issues.
18. See Appendix A.
19. https://www.mkm.ee/sites/default/files/records_management_metadata_en.pdf.
20. http://www.ra.ee/en/national-archives/.
21. http://www.ra.ee/vau/.
22. http://www.eark-project.com/ February 2014 to January 2017.
23. www.apex-project.eu.
24. http://4cproject.eu/.
25. https://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda-2020_Estonia_ENG.pdf.
26. https://www.mkm.ee/en/objectives-activities/information-society/records-management-information-governance. The information governance analysis and the strategic plan are being translated into English and will be available in 2015.
27. In January 2015 the National Archives published all its public archival descriptions at http://opendata.ra.ee/.

Transparency and Citizen Participation
Finland

Introduction

Government transparency, social inclusion, and public access to information are long-established traditions in Finland. The Swedish Access to Public Records Act of 1766, the oldest FOI law in the world, was applied in Finland while it was part of the Swedish Kingdom (until 1809). As early as 1859, the archives of the Finnish Senate, which evolved into the National Archives, were opened to the public. Finland's approach to social inclusion was evident as early as 1906, when it became the first nation in the world to give full sufferage to all adult citizens. Finland published its first explicit strategy for an information society in 1995, with an emphasis on quality of life, knowledge, and competitiveness.[1] When a new wave of transparency reforms began in the late 1990s, law and policy concerning transparency and secrecy were updated to enable private individuals to monitor public authorities' actions and expenditure, and the relationship between openness and the need for information management was articulated. In parallel, the National Archives began to develop practical guidance aimed at making information integrity and openness a reality in the digital environment.

Finland remained a largely agrarian country until the 1950s, but thereafter it developed rapidly as an advanced, industrialized economy, one of the strongest in Europe. Simultaneously, it built an extensive Nordic-style welfare state. In the 1990s, the structure of Finland's economy changed more profoundly than in any other OECD country in the same period. Finnish industry rapidly became technology-intensive, production became highly specialized driven by the information and communications sector, and Finland transformed itself into a knowledge economy. Finland's public administration successfully supported this remarkable transformation, and in the process it became a vehicle for economic development and service development, and for realizing Finnish values of social solidarity, eqality, and openness. Finland joined the European Union in 1995, and it was the only Nordic nation to adopt the Euro currency from its inception in 1999, although use began in 2002. Finland joined the Open Government Partnership in 2013 to work with others towards active citizen participation and open government. The cross cutting theme of its OGP National Action Plan is citizen participation.

Legal Framework

In Finland, public sector information management is a significant aspect of public adminstration and is guided by a series of interrelated laws. Underpinned by the Constitution, the principle of the openness of government activities and administrative processes as the basis for an informed and just society, runs through all of these laws. It is promoted and encouraged in particular through the Act of Openness of Government Activities, the Archives Act, and the Act on Information Management Governance in Public Administration.

CONSTITUTION OF FINLAND (731/1999)[2]

Section 12 of the Constitution notes specifically that documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings.

ARCHIVES ACT[3] (831/1994)

The Act specifies the duties of the National Archives as a government body under the Ministry of Education. It defines a record as a written or pictorial presentation that can be read, heard, or otherwise understood with the aid of technical equipment; it defines an archive as records received or produced by a records creator in the performance of its duties. The Act has wide coverage, including government offices at the national and municipal levels; courts of law and institutions applying the law; government and municipal enterprises; and collective bodies, organs, and persons carryings out public duties. The bodies covered include, for instance, the Bank of Finland, the Social Insurance Institute, some universities, and the Greek Orthodox Church of Finland and its congregations. The Act makes record creating agencies responsible for organising the practical aspects of records and archives management in relation to specific rules and regulations. Significantly, Section 7 of the Archives Law supports the right of private individuals and institutions to obtain information from records open to public inspection, provided that the legal rights and privacy are protected. The National Archives responsibilities are specified in closer detail in the Decree on the National Archives Service (832/1994).

FREEDOM OF INFORMATION LEGISLATION

Finland's long history of freedom of information legislation has evolved continually from the 18th century. There have been two principle acts.

Act on the Openness of Public Documents (83/1951). The Act established the openness of all records and documents in the possession of officials of the state, municipalities, and registered religious communities. Exceptions to the basic principle could only be made by law or by an executive order for specific enumerated reasons such as national security.

Act on the Openness of Government Activities (621/1999).[4] The act identifies the requirements for openness in relation to good information management practice in terms of availability, useability, integrity, and data protection. The Ministry of Justice is the responsible ministry. The act lays down provisions for access to information based on the principle that everyone has the right to official documents in the public domain unless prohibited by law, and any exception

must be justified. Secret documents and records include, for example, those concerning the Government Foreign Affairs Committee, criminal investigations, military intelligence, and state security. Decisions to withhold information can be appealed to an administrative court, the Chancellor of Judiciary, and the Parliamentary Ombudsman. Otherwise, the law specifies that the record normally should be provided within two weeks. However, the law is long and complex and can be difficult to apply, so legal experts sometimes have to be called in to interpret its application, and this can cause delays in providing documents.

The Act has a number of unusual features. It extends the principle of openness to corporations that perform legally mandated public duties, such as those relating to pension funds and public utilities. It identifies good practices in managing information, which is not typical for European laws, and it encourages the publication of government records as far as possible. It combines freedom to access and state secrets norms in one legal act. Authorities are obliged to provide information on matters that are in preparation, although this remains controversial. Europe's anticorruption commission has noted that effective freedom of information legislation in Finland is one of the key factors in low level of corruption in the country.

The Act is supported by the Decree on the Openness of Government Activities and on Good Practice in Information Management (1999).[5] The decree includes requirements for ensuring good practice in information management, right of access, obligation to disseminate information, and protection of personal data and sensitive data. It highlights the need to protect the usability, integrity and quality of data, particularly when used as the basis for decisions. It addresses risks for the availability, usability, quality and protection of data; for the security of information systems; for classification of specially protected information; and for access to information systems. It obliges authorities to prepare a description of the information system they maintain, indicating the purpose of the information system and the data contained therein.

ACT ON INFORMATION MANAGEMENT GOVERNANCE IN PUBLIC ADMINISTRATION (2011)

The Act gives the Ministry of Finance overall responsibility for steering information management in public sector authorities and for promoting and safeguarding public sector information technology interoperability and security across across sector borders to improve service provision. Public authorities are obliged to plan and specify their information governance strategies, and compliance is required to support effective access to information through administrative processes as well as to protect information integrity.

Administrative Framework

MINISTRY OF FINANCE

With the passage of the Act on Information Management Governance in Public Administration, the Minisistry of Finance took on a vital national role in steering information technology and information management, which it coordinates through a Public Sector ICT Unit. The Ministry also set up several advisory bodies: an Advisory Committee on Public Sector Information Management, an IT Coordination Group, and a Government Information Security Management Board. These bodies have played an important role in coordinating development, information

exchange, and networked collaboration. Cooperation in the field of government information security is considered to have been particularly successful.

With the increase of information networks in all public services, there has been a growing emphasis on harmonizing operational procedures across the public administration through an overall information management architecture and by providing common structures for information systems. A common Public Sector ICT Strategy for central and local government was developed by 2012[6] led by the Ministry of Finance with cross-government input. The focus is on customer oriented public services, good IT governance, interoperable processes, reuse of public sector information, harmonized ICT infrastructure, data security, and fully functional government in all circumstances.

The aim is to develop seamless but flexible cooperation between public sector managers and senior information personnel in managing information to facilitate evidence-based cross-organizational service provision and to break down policy silos and fragmentation between institutions. Finland's approach emphasizes open information, effective information management, and evolving technological solutions. It includes safeguarding the reliability of the public sector and trust in public services by investing in data protection, information security, and contingency planning. It also identifies the need for joint use of information through clear information management structures and a reliable cost effective ICT infrastructure. The intention is that information and communications technology should become an everyday part of municipalities' and authorities' operations and management.

The Ministry of Finance is responsible for issuing Public Administration Regulations (JHS regulations) on ICT information management to state and municipal agencies. A JHS Regulation can be a uniform procedure, definition, or instruction to be used in public administration. The JHS system aims to improve the interoperability of information systems and the compatibility of data within them, to facilitate cross-sector process development, and to make the use of existing data more efficient. The recommendations also aim to minimize overlapping development work, guide the development of information systems and facilitate good common practices in public administration. The aim is to ensure that that Finland's public sector information systems and networks work together to support efficiency and quality in terms of interoperability, processes and procedures, data and data structures, architectures and ecosystems, information policy, access to information, open data, and data reuse. There are JHS Regulations covering aspects of digital records and data management, including registering, keeping, handling, retrieving, and transferring documents; email; and IT procurement.

Led by the Ministry of Finance, the Open Data Programme (May 2013 to June 2015) has been working to eliminate obstacles to reusing of public data and to create the preconditions for making data open within the public administration. A range of organizations, including state government ministries and government agencies, municipal governments, enterprises, NGO's, and citizen bodies are collaborating to implement the program. Moreover, a systematic process for opening data has been adopted as a part of the budgetary framework process. Since 2012, the Ministry of Finance has asked ministries to draw up and submit plans for open data and to assess the impacts on the budgetary framework. The goal is to develop a systematic process for releasing open data.

In addition, open data is being linked to work on enterprise and information architecture emerging from the the Act on Information Management Governance in Public Administration.

The approach is that rules and practices for public sector information integrity and longevity should be applied to open data. At present, there are no special measures for managing open data through time, but the Ministry is starting a project on common long-term data archiving services for public sector. Open data, which is released through Finland's open data portal,[7] must be re-usable, free of charge, machine-readable, and licenced openly. The Ministry of Finance has issued a JHS Regulation indicating that public sector agencies should use the Creative Commons 4.0 BY as the licence for open data.

The Ministry of Finance has launched a program (2014 to 2017) to create a uniform National Digital Services Architecture to support interoperability between services, databases, and information registers. This includes building a National Data Exchange Layer that will integrate information systems and should be in production by the end of 2015. Finland is cooperating closely with Estonia, with which it shares a commitment to digital governance reform aimed at maximizing service provision.[8] Estonia's X-Road technology, which enables different information systems to exchange data safely via the Internet, also will be used in Finland. The aim is that Estonia and Finland will work together to develop X-Road further in the future.

NATIONAL ARCHIVES

The National Archives has been responsible for the memory of the nation since 1816, when it was created as part of the Senate of Finland. It became a central government agency in its own right in 1939. Today, under the Ministry of Education and Culture, it coordinates seven provincial archives as regional administrative authorities. The Archives' responsibilities include determining the value of the records of state authorities as permanent archives, disposing of those without ongoing value, preserving and making available those of long term national signifance, and providing research and information services. It also obtains and preserves private archives of importance for society. It operates an extensive program to digitize documents for permanent storage and preservation as a Digital Archive. Digitization began in 2009, and by 2013, there were over 18 million files in the Digital Archive, a number that continues to grow steadily.[9]

The National Archives' broad remit for preserving the memory of the nation inevitably includes playing a key role in protecting and preserving information integrity in the digital environment, where decisions at the point of creation affect the ability to manage the records and data and to preserve and use them through time. Although the Archives law was enacted in 1994, before it was imperative to address digital issues, the Archives is committed to protecting the integrity, authenticy, and accessibility of essential public records in digital format. It recognizes the importance of managing digital information consistently from the point of creation, and consequently it has developed in-depth knowledge and specialized skills in defining and documenting content and context and in managing long-term digital preservation.

International standards and operating practices play an ever more important role in planning and executing the Archives' operations, making its contribution to managing information in the in the information society increasingly vital. It contributes not only in terms of its high quality preservation services but of its specialized understanding of the management controls needed to protect the quality, integrity, and longevity of digital information, and access to it. The Archives' active participation in regional and international professional activities creates opportunities for developing and continuously upgrading information and storage systems. The close

collaboration between national archives in the region means that strategies are continously enriched through shared experiences.

Life cycle planning, or the continuum of management responsibility for records and data from the point of creation, is at the core of Finnish records management just as it is for international good practice. Extensive international collaborative work on professional standards has demonstrated consistently that this is the safest and most effective means of establishing and retaining control of the quality, authenticity, and trustworthiness of public sector records. The National Archives has successfully related this understanding to public administration requirements.

Traditionally, Finnish record keeping was achieved through registry systems that enabled metadata capture for incoming and outgoing records in registers. The principle of registration and metadata capture remains central to Finland's digital records management strategy. When a record is registered, it is linked to an an aministrative process. Everything that comes into and leaves a government agency goes through the registry office and is recorded. Registry officers, who tend to be very well educated, make sure that no electronic record goes through the registry without being attached to an Electronic Document and Records Management System (EDRMS). Registration captures information about what 'cases' are open, what actions that have been taken in any particular case, and what records have been created as a result of these actions. This supports the ability to trace records required for Freedom of Information requests and to demonstrate transparency and accountability. The National Archives has been offering education and guidance to public sector agencies on lifecycle/ continuum management for records and data, including issues of secrecy and openness. This has helped to address concerns by staff in government agencies who do not yet fully trust digital information and are worried that it will not be possible to preserve it permanently.

At present, the National Archives has statutory authority to issue detailed and binding regulations for managing records and metadata of permanent value to the nation across state and municipal public sector agencies in the context of electronic services and communications. Its SÄHKE Records Management Standard, and the closely related VAPA Service for receiving and storing digital records and data, are particularly important contributions to the ability to demonstrate an unbroken chain of custody and demonstrate authenticity.

SÄHKE Records Management Standard

As early as 2001, the National Archives initiated the SÄHKE project to define a framework for managing records produced by electronic records management systems (ERMS). The requirements were published in 2005 as the SÄHKE Standard, which came into force in 2006. The current version, the SÄHKE2 Standard, was published in 2009.

Government authorities determine their own approach to managing their digital records and data but are required to use SÄHKE-compatible digital records management systems if they want to preserve records with permanent value in electronic form. The National Archives determines which public records and data are to be preserved permanently, about 10 to 15% of all public authority records. The longer term aim is to keep much more and to preserve complete record systems, registries, and databases. In 2010, the Ministry of Finance led an attempt to build common records management systems but was not successful because ministries felt that their needs were unique and wanted to make their own rules about how their records and data

were managed. The Archives now is encouraging common systems within each ministry and the agencies under it.

The SÄHKE requirements concentrate on building and maintaining records management schedules and associated metadata. They provide a set of record-keeping metadata elements, with defined metadata fields, to enable a standardized approach to capturing and describing content and context as a basis for access control, usability, integrity, and authenticity, and for managing secrecy and openness. The requirements specify that each authority must have a records management schedule defining arrangements for registration, filing, and retention. Far more than a passive list of retention periods, the schedules are in effect life cycle plans. Public authorities must determine how long the records need to be retained so that they will not need to be appraised afterwards. As far as possible, the system assigns the metadata automatically, guided by default values in the records management schedule.

The SÄHKE requirements are unique to Finland, but they were not developed in isolation. Early work on the de facto European standard, MoReq,[10] provided a source for SÄHKE development, although there was no intention to produce a MoReq compatible regulation. The two standards use different data models, elements, and functional requirements, but both set requirements for functionality and metadata in Electronic Records Management systems and both define an a XML-scheme for exporting records from information systems.

The Archives has developed an interface for consistently transferring digital records to long term custody from diverse electronic records management systems. This involves a standards compliant delivery check using the SÄHKE2 metadata model. The standard also acts as an accreditation framework for electronic storage systems, and suppliers of systems can apply for a SÄHKE compliance certificate.

VAPA Service

In 2011, the National Archives launched the VAPA service for receiving and storing digital records and data identified as having permanent value. Free of charge for government organistions, the service is intended to safeguard the storage of digital materials reliably and securely for several centuries through changing technologies. Ultimately, the aim is to extend the storage facility to cover the entire public administration enabling smooth transfers to the Archives' repository. VAPA, which complies with the internationally accepted OAIS specification,[11] supports essential preservation functions, including ingest, archival storage, data management, access, and dissemination. It also defines digital preservation responsibilities for organizations. It can be adapted to changing circumstances and upgrade paths, and modular components can be added flexibly as required.

VAPA is harmonized with SÄHKE2. Record and data creating agencies develop submission information packages as defined by the standard and send them to VAPA. SÄHKE structured metadata and accepted file formats are validated automatically in the ingest workflow, and signatures and checksums are used to ensure the integrity of the information. The material is safeguarded against viruses and unwanted access and alteration, with firewalls protecting government servers and access channels being secured through cryptography. Digital signatures are decrypted at the point of ingest, as it would be impossible to update and renew certificates for the growing number of documents. However, the information in the digital signature is documented in metadata, which is transferred to digital storage with the document.

Database Management

Thousands of registers and databases had been maintained in the public administration over the last several decades, often to support official functions, such as personnel administration. Large national databases and registers have provided unique source material for studying macro-level effects and complex causal questions. However, much if not most of this information has not been protected and systematically preserved and is at risk of being lost inadvertently.

In 2012, in response to a growing demand for solutions to preserving information in databases, the National Archives began developing techniques, tools, methods, and practices for ensuring and protecting the authenticity, integrity, and usability of information in databases and registers. It started by studying relevant international standards and good practices. Notably, it drew on the Swiss Federal Archives' SIARD-standard (Software Independent Archiving of Relational Databases), a widely used standard in database preservation, and on the Norwegian Archival Service's standard for technical metadata, ADDML (Archival Data Description Markup Language). ADDML is used to describe data files such as tables, fields, variables, codes, their relationships and their meaning by providing a technical and structural data description in standardized format. Finland's National Archives is cooperating with the Norwegian and Swedish National Archives to continue developing the ADDML standard.

Preserving databases presents a range of challenges. Databases are generally used for several years and updated regularly. They usually are not self-documenting, and without accurate and consistent metadata and contextual information, the data can be unclear and may have little or no value. If a database has been in operation for a long period, fields and codes may have changed, and older data may differ from newer data. Frequently, database documentation does not include information about changes. Older data are often poorly described, and documentation may be completely lost or available only in paper format. Moreover, many databases are maintained jointly by several authorities, although still owned by a single office, and this can make documentation difficult to trace. Preserving databases requires a description of the database along with the obligatory metadata elements needed to understand the data, including its content, the context of its creation and use, its classification structure, and any restrictions.

The Archives strategy is to preserve the data and its description, but not its functionalities or data processing rules and algorithms. The data is extracted from a database and converted to XML or CVS format, and the ADDML standard is applied. The binary images extracted from the database are converted to PDF/A format[12] and preserved. Documentation covering the context, data origin, database management system, data models, processing rules, and usability guidelines is described using a standardized structure and metadata, as defined in SÄHKE2. It is attached as an integral part of the submission package and preserved with the data to support future users needs. At present, the Archives only accessions older databases, where data is no longer altered, and these are not yet publicly available. However, this is an area where the Archives' investment of time and expertise will have significant benefits on the future.

Challenges

The primary challenge for managing information in the digital environment in Finland is the need to clarify management responsibility. At present, the management of digital records and data is governed by several different laws enacted over the last 20 years and by guidance from three different ministries: Finance, Education, and Justice. Because of this, the relationshhips, roles and responsibilities of the different authorities involved, particularly the Ministry of Finance and the National Archives, tend to overlap and to be unclear. There is collaboration, but the structure does not yet support a unified strategy. The challenges of managing and preserving digital information require a new model to define how the strengths of the agencies involved can come together as part of a holistic approach.

For this reason, an initiative is under way to develop a new act that will cover the entire lifecycle or coninuum or information. Initially, the focus was on revising the Archives Act, but it has become clear that a new act is needed to introduce a coordinated approach to information management across state and municipalitity authorities in relation to goals for openness and digital governance. The aim now is to combine and harmonize the different laws and regulations concerning information management, including provisions for access rights. Finland follows the principle that international standards should be used where they exist, and the new law will provide a basis for harmonizing relevant standards, for instance those for interoperability and security and for records and data management.

Under the new law, the Archives' role in defining requirements will change. There has been concern that the SÄHKE Standard is in some senses too demanding, for example when applied in the municipalities, and that it should be effectively harmonized with all aspects of digital governace. The standard is, therefore, being re-examined as part of the process of redesigning the approach to information management. From the end of 2015, the Archives no longer will have the power to prescribe the SÄHKE2. After that, records and data management will be defined through the JHS Regulations issued through the Ministry of Finance. It is not yet clear how the VAPA service will be managed.

A Public Sector Recommendation, JHS 176, will replace SÄHKE. The JHS 176 Working Group is defining the functional requirements for an ERMS, including how to build systems and how to transfer or destroy records. It also will deal to a a certain extent with open data issues, including data and its preservation, particularly personal data. In addition, the issue of record secrecy and openness, central to the SÄHKE2 standard, and will be an essential part of the JHS 176 regulation. National Archives staff, whose indepth expertise in international good practice and experience of the practical realities of managing, accessing, and preserving digital records and data, will have an invaluable contribution to make, and their input has been welcomed. Once the new regulation is accepted and formalised as a standard, it may become a decree. Given the powerful role of the Ministry of Finance, the scope and contribution of records and data management controls could be greatly enhanced.

Conclusion

Finland views information management as an integral aspect of its approach to maximizing the opportunities of digital government and enabling openness. Its network of information management-related laws contributes fundamentally to its ability to deliver its values of social solidarity and equality in a technically complex digital environment. Finland is now in the process of harmonising its laws and practices for managing records and data in relation to its goals for customer oriented public services, good IT governance, interoperable processes and services, reuse of public sector information, and data security. Its aim is to facilitate evidence-based cross organizational service provision.

As part of the process, the roles of the Ministry of Finance, the National Archives, and the Ministry of Justice are being harmonized and reconfigured to draw on their mutually complementary expertise in the areas of ICT development, information integrity and access, and social justice. Finland's innovative approach to developing a new model for information management highlights the need for a fresh approach to meeting the challenges of protecting and preserving high quality information in the digital environment and for maximizing its value for citizens. All countries will need to address this essential issue if goals for digital governance and openness are to succeed, and Finland's bold approach will demonstrate the opportunities for change.

Notes

1. http://e.finland.fi/netcomm/news/showarticle7dfc.html?intNWSAID=9989.
2. http://www.finlex.fi/en/laki/kaannokset/1999/en19990731.pdf.
3. http://www.arkisto.fi/uploads/Arkistolaitos/Tehtävät%20ja%20toiminta/The-Archives-Act-831.pdf.
4. http://www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf.
5. http://www.finlex.fi/fi/laki/kaannokset/1999/en19991030.pdf.
6. http://www.slideshare.net/mikaelvakkari/public-sector-ict-strategy.
7. See a catalog of open public sector datasets at avoindata.fi.
8. OECD Public Governance Reviews Finland: Fostering Strategic Capacity across Governments and Digital Services across Borders, March 2015, http://vm.fi/documents/10623/1107144/key-findings-finland.pdf/b991582d-fc08-4b0c-b57f-21bea5e6eb3f.
9. http://digi.narc.fi/digi/?lang=en_US.
10. MoReq® is a records management specification of modular requirements for electronic/ digital records systems. First published in 2008 by the DLM Forum, a European wide organization of national archives, enterprises and research organizations with an interest in electronic records management, it is intended for users and suppliers of electronic records management systems and services, and for educators. It can also be used to provide a basis for auditing existing electronic records management systems or services, and as a resource for academic or commercial trainers. The latest edition of the MoReq® specification is MoReq2010®. See http://moreq.info.
11. The OAIS reference model (ISO 14721:2003) addresses a full range of archival information preservation functions including ingest, archival storage, data management, access, and dissemination. It also addresses the migration of digital information to new media and forms, the data models used to represent the information, the role of software in information preservation, and the exchange of digital information among archives. It identifies both internal and external interfaces to the archive functions, and it identifies a number of high-level services at these interfaces. See http://www.iso.org/iso/catalogue_detail.htm?csnumber=24683
12. PDF/A is an ISO-standardized version of the Portable Document Format (PDF) used for the preserving digital documents. It identifies a 'profile' that ensures that the documents can be reproduced consistently in years to come. A key requirement is for PDF/A documents to be 100% self-contained; all of the information necessary for displaying the document in the same manner is embedded in the file.

Information Integrity and Access to Information

Norway

Introduction

Norway, one of the most open governments in the world, has achieved a remarkably high degree of information integrity and accessibility in the digital environment. In common with other Nordic countries, Norway's aim is to make government as accountable, transparent, and democratic as possible. Its comprehensive national ICT policy, launched in 2000, makes using information technology effectively a national priority, and its long term commitment to managing digital information, makes it possible to use the records and data produced by digital systems as high quality evidence for making decisions, providing services, and empowering citizens through a unique and advanced approach to Freedom of Information/ Right to Information. Norway was the first country, in 1984, to define and implement a fixed set of model requirements for managing digital information systems.

Norway's leading edge approach to openness is achieved through a powerful combination of interconnected laws, standards, well-defined metadata architectures, and technology systems. Among the most striking aspects of its approach are the emphasis on protecting the security, content, and context of the information, and on reducing the time between creating records and public access. This has enabled Norway, through right to information laws and policies, to give its citizens rapid, almost real time, access to reliable records as evidence of policies, actions, activities, and expenditure, making openness real and concrete, not just a vision for the future. Norway's citizens are able to monitor what their government is doing, claim their rights effectively, and play a significant role in influencing the affairs of state. Journalists can regularly track and report on what the government is doing on the basis of in-depth, reliable, and readily available evidence. Public sector agencies are able to plan and monitor programs, activities, and expenditure on the basis of consistently trustworthy information and citizen feedback.

Norway was one of the eight Open Government Partnership founding members. Norway's action planning for open government has emphasized the necessity for financial openness in connection with income from the petroleum sector. In addition Norway has been committed to sharing knowledge on, and experiences of, developing an open and well functioning public sector. In the next phase of its OGP Action Plan, Norway will follow up in areas including improving access to information, facilitating democratic participation in government, and enhancing fiscal transparency and financial integrity.

Legal Framework

The Constitution, the National Archives Act, and the Freedom of Information Act work together to provide the legal basis for Norway's unique and powerful approach to right to information and the means of ensuring transparent evidence-based government.

CONSTITUTION

Adopted in 1814, Norway's consitution is the second oldest written constitution in the world. Founded on the principles of sovereignty of the people, separation of powers, and human rights, the constitution has been amended over the years to reflect an ever-deepening commitment to openness and transparency. In the most recent version, adopted in 2014 at the Constitution's bicentenary, Article 100 emphasizes citizens' right to trustworthy information:

Everyone has a right of access to documents of the State and municipalities and a right to follow the proceedings of the courts and democratically elected bodies. Limitations to this right may be prescribed by law to protect the privacy of the individual or for other weighty reasons. The authorities of the state shall create conditions that facilitate open and enlightened public discourse.[1]

NATIONAL ARCHIVES ACT

Norway's National Archives, established in 1817, is almost as old as the constitution. In Norway, 'archives' means the whole lifecycle of the records, from the point of creation through to preservation and future access. The Archives Act of 1992 sets out the National Archives' responsibilities for overseeing the creation, management, and preservation of records, in any form, that document public institutions' functions and exercise of authority; provide information of general interest to society; and document the obligations and privileges of people and organizations. The Archives Act requires public organisations to register all incoming, outgoing records, and internal records that generate or document official activity, in a national records management system, 'Noark'.

FREEDOM OF INFORMATION ACT

The Act Relating to Public Access to Documents in the Public Administration (the Freedom of Information Act) (1970) mandated that case documents of the public administration were public insofar as no exception was made by or pursuant to statute. Any person could demand to be apprised of the publicly disclosable contents of the documents in a specific case. Government administrative agencies were required to keep registers pursuant to the provisions of the Archives Act and its regulations.

The Act Relating to the Right of Access to Documents Held by Public Authorities and Public Undertakings (the Freedom of Information Act) (2006) established the basic principle that everyone has the right to access to state and municipal documents unless the records are legally restricted by this or another act, for instance the National Security Law, Personal Data Act, the Environmental Information Act, or the Public Administration Act. The law requires all government adminstrative agencies at the state, county, and municipal levels, unless exempted from

the Act, to make case documents,[2] journals and similar registers, and email publically available for access, as soon as they are produced, received, or transmitted, available to the public by the means of an electronic journal available on the Internet, pursuent to the rules of the Archives Act and associated regulations.

Administrative Framework

NATIONAL ARCHIVES

Noark Standard

In the 1980s, the National Archives, working in collaboration with the Governmental Rationalization Directorate,[3] recognized the importance of managing digital records as evidence and began to define good practice requirements. First introduced in 1984, the Norwegian Model Requirements for Electronic Records Management Systems (Noark), have evolved to structure the way government agencies capture, protect, and provide access to official records in digital form. When Noark was launched, the National Archives also introduced 'Guidelines for Implementing Computerized Registering Systems' and 'Instructions for Records Management in the Governmental Sector'. Initially, the Rationalisation Directorate was legally responsible for Noark, and Noark 2, published in 1987, was also a result of collaboration between the Archives and the Directorate. Responsibility for Noark was transferred to the Archives in 1990.

As was the case in many European countries, public sector records in Norway had long been managed through registry systems that captured metadata about incoming and outgoing correspondence and gave the records their legal authority. Once registered, records could not be altered without authorization and evidence of change. From the outset, the Noark Standard used the concept of metadata management, which was already established in Norwegian law, as the foundation for building information integrity. Noark mirrored principles defined in the Norwegian Governance Act (1967) and the Norwegian Freedom of Information Act (1970), which together defined a set of core metadata elements (date of registration, record number, sender/recipient information, description of content or subject, document date, classification code, date, and method of processing). The first version of Noark retained and broadened these metadata elements to support integrity in government systems.

Under the Freedom of Information Act of 1970, each government agency was required to produce a public register ('offentlig postjournal') of metadata for incoming and outgoing documents, and from the beginning, Noark included a records system requirement to generate a public register electronically. Not only did this provide a basis for locating digital records and protecting their integrity, but the registers were printed and made available through government press centers, marking a major step toward transparency. Noark and the public register, both of which are fundamental to Norway's approach to the right to information, were twinned developments from the outset.

Noark was not mandatory for government agencies until 1999, but it quickly became a de facto standard for Electronic Document and Records Management Systems (EDRMS) for government bodies. Noark compliant systems were recognised as having better functionality and stability than other records and document systems, and long before Noark became mandatory, records created in government agencies were largely compliant with the Noark requirements. By

1990, when responsibility for the Noark Standard was transferred to the National Archives, more than 90 government institutions, including all ministries, were using Noark-systems.

As it developed, Noark secured the principles of governance, transparency, and predictability by setting requirements for fixity, predictability, consistency, traceability, and searchability. The resulting consistency, including the common set of metadata, has enabled a standardised approach to public access to government information. The launch of Noark 3 in 1994 marked another major step toward transparency. Now the mandatory public register of metadata was uploaded regularly from government agencies to a web-based, password-protected platform known as the Electronic Records Registry (EPJ). This made it possible to provide newspapers and television agencies with regular access to public information.

Noark 4, introduced in 1999, specified a complete, mandatory electronic records management system, integrated with e-mail and general case handling systems. It now became mandatory for public bodies to use a Noark-based system for electronic recordkeeping. Once the government endorsed the Noark Standard, vendors were permitted to sell only Noark compliant electronic records and archives systems in the public sector. After Noark 4 was launched in 1999, the Archives began to supervise digital recordkeeping, working with IT departments and vendors, to support Noark compliance.

Until Noark 5 was introduced in 2008, government agencies with non-standardized systems did not have to comply with Noark. These included large nationwide systems such as those operated by the Bureau of Statistics and the National Tax Authority. Little was known about the content or the structure of these systems, making it very difficult to trace and capture the relationship between metadata and records and to preserve it systematically; a lot of information was lost or later became inaccessible. Noark 5 defines a core of minimal mandatory requirements for records structure, metadata, and functionality. It does not specify how these requirements should be met in system development, but it does require that obligatory metadata be included when records are exported from a records system and that the extraction must follow a defined structure. Extraction from the non-standardized systems is possible using the Archival Data Description Mark-Up Language (ADDML), a de facto standard for developing technical and structural data descriptions as flat files.[4]

The Noark requirements have evolved steadily in response to the growth of electronic communication between public sector agencies and between them and the public, across sectors and regions. The National Archives has taken a highly practical and pragmatic approach to Noark development. Its computer engineers and records professionals work from their different perspectives to define and address the challenges of capturing and preserving trustworthy records in relation to constantly changing developments in platform complexity, system portfolios, and functionalities. The Archives works closely with international colleagues and staff in government agencies to ensure that the Standard takes account of international good practice and practical needs. This farsighted approach continues to evolve and to remain at the cutting edge of international good practice for ongoing access to high quality information.

The Noark requirements have a range of benefits for users across government. The pre-defined structure for capturing context and content means that information elements and objects follow a predictable pattern that essentially eliminates unauthorised deletion, alteration, or manipulation of metadata and documents in government organisations. They make it possible to rapidly retrieve, disclose, present, and communicate high quality evidence of government policies, practices, and transactions across the public sector, enabling public sector agencies to plan and monitor programs, activities, and expenditure effectively. For instance, it would be

possible to determine how many records are pending decisions, and to identify cases similar in nature that require similar actions, thus supporting the principles of precedence and common practice. In addition, the requirements describe routines for security backups and support recovery functions when there is interference such as a hardware failure or a powercut, making government information continuously available.

Trusted Digital Repository

In 2009, the National Archives launched a project to develop a digital repository system that would meet the highest level of international good practice based on the principles of international IT security and appropriate elements of the Open Archival Information System (OAIS)[5] and the Trusted Repository Audit and Certification Checklist.[6] The aim was to secure contextual authenticity, making it possible to demonstrate that what is stored in the repository has the same structure and relationships as what was produced in the creating agencies. At the beginning of 2014, the Archives launched an open source Trusted Digital Repository system, developed by a Swedish supplier and adapted for national and municipal use in Norway. This provides a technology-neutral means of preserving public sector records using standardised digital preservation models. The system also is implemented in the National Archives of Sweden.

Legally, records and associated metadata must be transferred to the National Archives digital repository after 25 to 30 years. However most central governmental agencies make submissions when a new EDRMS is introduced or when organizational changes require an alteration of the classification system, generally within ten years of the record's creation. Transfers include structured extractions from the Noark databases in government agencies, including the associated metadata and relational context logs documenting records' creation and any subsequent alterations. This audit trail of context or changes in status enables traceability and helps ensure that the records continue to meet legal, administrative, fiscal, or other evidentiary needs through time. The metadata, which is structured according to Noark and is compliant with other international metadata standards such as Mets, Premis, Mix, EAD and EAC, also provides the means of locating, interpreting, and interrelating the information, and of facilitating migration and conversion to new formats and software and hardware environments as necessary.

Records and metadata transferred to the digital repository pass through a validation process to ensure that the submission package complies with the and digital signatures are removed as precribed in the Archives Act. The Archives uses checksums to ensure that the records in the submission package have not been altered. It holds the transferred material in quarantine while it performs extensive virus-scans before the transfer is formally brought into the repository.

At present, there is limited access to recent digital information held in the Archives repository, which is still used primarily to make digitized historical documents available, although some of the earlier Noark submissions can be accessed. This is partly because if any records in a series are closed under Freedom of Information restrictions, the entire series is closed and is likely to remain closed until all the records in the series can be opened. It is also because there are time lags in accessioning records from government agencies. In the future, there are significant opportunities for sharing digital records through the Archives' repository. For instance, in 2011 and 2012, the Archives developed two smartphone apps for access to its holdings, creating the possibility that the repository could eventually become a public transparency portal for digital records and data through smartphones and other mobile devices.

OEP (OFFENTLIG ELEKTRONISK POSTJOURNAL)

Norway's revised Freedom of Information Act of 2006, implemented in 2009, took access to information to a new level. Rooted in a commitment to protect transparency and citizens' rights through access to public sector information, the law required government agencies to upload, daily, standardized metadata for incoming and outgoing documents to the Electronic Records Registry. The Registry was updated with advice from the Norwegian Press Association and re-launched in May 2010 by the Agency for Public Management and e-Government, the Directorate for Governance and ICT (Difi) as the OEP.[7] The OEP searchable database is no longer password protected and can be used by anyone, anywhere in the world, who has Internet access. All that is needed is a description of the information wanted.

Managers and case handlers[8] in government agencies must ensure that everything that can be opened is opened. This involves a high level of scrutiny, and normally the section head or an adviser makes a final check. Records are tagged to prevent publication of metadata where there is a legal restriction on publication, and without exception, sensitive personal information is masked, for example, information about an individual's health, personal finances, or criminal record. About one fifth of the records are classified for security reasons and are not listed in the register.

The OEP, which has become a core part of the Norwegian Government's approach to transparency and democracy in the public sector, has enabled a remarkably generous degree of openness unknown elsewhere. It is a powerful tool for providing access to public records online by enabling searches across all state public sector agencies, which use common search terms. It is easy, for instance, to access records regarding an event, a political incident, or expenditure in areas such as as fisheries, health, or the oil industry. The most common search terms used are report, complaint, inspection, demand, revision, supervision, deviation, work accident, evaluation, illegal, and allotment letter.

Having located relevant records, users submit FOI access requests through the OEP, which forwards requests to the responsible agencies. The agencies have five days to respond to information requests, but they often reply within two or three days. They send copies of the records to the users by email, fax or regular mail, often choosing to provide not just the one document requested but also related documents. There are no restrictions on reuse and there is no charge. Citizens can appeal any refusal of information or partial release by approaching the agency immediately superior to the agency from which the information was requested. The agency has ten days to justify refusal. Failure to respond to an appeal can result in a complaint to the Parliamentary Ombudsman.

The OEP provides a very significant tool for the press in Norway, enabling journalists to track the way public authorities develop and implement public policy and to keep the public informed.[9] The Norwegian Press Association's Freedom of Information Commitee even provides a website called called offentlighet.no (freedomofinformation.no),[10] with a link directly to the OEP.

By the end of 2012, the OEP contained over five million registry entries published by 105 government agencies. The OEP was processing about 20,000 information requests a month, with the greatest number of requests coming from journalists (50%); citizens and businesses made up 22% of requests, public employees 21%, and researchers 3%.[11] The Government is considering the possibility of providing direct access to digital records direct from the OEP with the aim of making administration more open and transparent and enabling government agencies to

work more efficiently. The Norwegian Press Association, which continues to work with the OEP management, supports the goals of publishing entire documents on the OEP and extending OEP requirements to municipalities, which are not covered at present. There is no direct link from the OEP database to the Archives' digital repository, but this may be possible in the future.

Challenges

Although Norway has achieved an unparalleled level of information transparency, the National Archives faces immense challenges in its ongoing efforts to manage and preserve digital records. Norway's digital agenda calls for common solutions for digital governance in public administration, with digital communication as the basis for management. In this rapidly changing environment, the Archives' administrative positioning is a crucial factor in its ability to contribute its immense knowledge and experience to national aims for sharing information more efficiently and providing enhanced digital services.

The National Archives is part of the Ministry of Culture. While preserving culture is one of its legal responsibilities, protecting 'rights documentation' is another. In the past, the emphasis was on serving the needs of historical researchers rather than on supporting transparency and public services. Today these priorities are changing, not only to enable good e-governace but also to ensure that an historical and cultural record will survive for the future. Enabling accountability, monitoring state performance, and supporting citizens' rights and needs requires that digital information should be managed in as an aspect of digital governance, which is the responsibility of the Ministry of Modernisation. There is a need for a new approach to roles, responsibilities, and strategies. It is significant that the Archives has been included on some of the boards working on new e-governance solutions and architecture, and that Norway's National Archivist comes from the electronic governance sector. The National Archives will be performing a detailed mapping of electronic systems in all 3500 state government agencies in 2015, which should provide valuable information for planning purposes.

The principal challenges are to develop and implement new strategies for protecting and preserving public sector digital information, extending access to it, and incorporating interoperability functionality in Noark 6, which is already being planned. The issue of email, which is increasingly urgent as more and more of the official workflow is conducted by email, also needs to be addressed in the new version of the Standard. In theory all email into and out of government agencies is to be captured in the Noark system, with metadata recorded as for other documents and available through the OEP. However, capture is not automated as part of agency records systems, and often employees do not want to spend time registering email. This thorny issue was emphasized in the 2015 report of the national SAMDOK Project, (The Consistent Documentation of Society Project) coordinated by the National Archives, and there is increasing recognition of the importance of addressing it.[12]

One of the most significant challenges is the difficulty of making transfers from record creating agencies to the National Archives' secure digital repository. Agreements on transfer are worked out through appraisal negotiations when an extraction is agreed. These negotiations may not happen for several years after the records are created, but even when they do, the agencies and the Archives have limited capacity to follow up, and there can be a further long gap before the transfer actually occurs. There are cases where records are up to 15 years old before they transferred. The result is that a large backlog of digital records and databases remain on agency

servers, where there is a diminishing ability to protect their integrity and preserve them as time passes and errors in their description become increasingly difficult to rectify.

The primary reason for the delays is the scale of effort and cost involved in extracting and transferring records from record creating systems to the National Archives. Creating a submission information package compliant with Noark requirements is difficult and time consuming. There are approximately 3500 record creating agencies at the state level, each with a digital records system. The time and skill level required to carry out an extraction is so great that Noark system vendors or consultancy firms have to be hired to do the work at a high cost. The process is particularly time consuming and technically difficult where specialized systems are not Noark compliant.

Over the last several years, the search for solutions has stimulated new questions about the systems needed to extract and protect the quality and authenticity of records created in government agencies.[13] It has become increasingly clear that there is a critical need for a simpler, cheaper automated means of extracting the records and metadata in such a way that it can be used effectively to benefit society. The approach needs to be easy to apply, so that even those with little or no IT competence can make an extraction and wrap it in data description markup language to structure the metadata and make it possible for the records and databases to searched and used reliably in the future. The proposed solution is to develop an intermediate eArchive, linked to the long-term digital repository, or to clusters of repositories. The Archives' projected timeframe is 2015 to 2018.[14] Funding is not yet adequate to fully develop the new framework and associated tools, but hopefully as the benefits become clear, progress will be more rapid.

Creating the eArkive will involve building a standardized application programing interface, linked an upgraded Noark 6, to enable continuous mandatory data transmission from the creating agencies to the eArkive. The eArkive will enable the Archives offer timely guidance and meaningful feedback on the means of rectifying systemic errors while staff still are familiar with content and before the errors multiply. Simplifying and streamlining processes will prevent long delays in bringing records and data into secure custody, minimize the risk of lost records and data, and greatly reducing the costs involved in maintaining digital records in government agencies and in supporting extraction. The result will be that higher quality records and data are available earlier for research and that they survive through time. The eArkive also will support enhanced interoperability and the ability to share information between public aencies. The fact that Noark is a mandatory standard across state public administration agencies will mean that changes can be effected much more quickly than would be possibile in an unstandardized environment. The eArchive, based on Noark requirements, also could remove regulatory obstacles to the use of the cloud, since digital information could potentially be held in a public sector cloud secured on Norwegian soil under government control.

Significantly, in terms of openness, the eArchive will make it possible to greatly enhance the OEP. Difi has received funding for a pilot project to evaluate a new OEP solution, and the National Archives and the OEP team have been exploring collaboration. The eArchive architecture could be planned to intersect with a new OEP solution, based on an upgraded Noark core, to support much enhanced access to records, and hence enhanced transparency and accountability. The Archives is beginning to explore ways of structuring its repositories in line with OEP architecture, with a view to making documents, as opposed to simply metadata, available automatically. This could provide a model for making material in repositories easily accessible online. The benefits for the OEP would be lower costs of publishing the documents, a greatly enhanced

ability to support openness and management transparency, and the ability to protect and access records and data through time.

Municipal and county governments face similar but more challenging issues: there are few resources for preserving digital records, with only a handful of technicians around the country with extraction competence, and few digital repository facilities. The backlog of unsecured records is far greater than at the state level.[15] Some bigger cities have or share repositories, but mostly for paper records. A digital resource centre in Trondheim is intended to play a national role, but has not yet implemented a digital repository system. Many municipalities want the National Archives to take responsibility for their records, but the Archives does not have the resources to do this, and in any case, innovative work is already underway in large municipalities, including Oslo, Bergen, and Trondheim as well as in the smaller municipality of Kongsberg, including work on making metadata and entire documents available on public websites. There would be real value in collaboration between the state and municipal levels in developing the eArchive.

Sweden is developing a similar solution, which is to be introduced in several major government agencies in 2016, with the aim of achieving cost savings, more efficient public management, and better protection of digital information that has legal, administrative, and historical significance. Although the two systems are different, experiences from Sweden will be valuable in developing the Norwegian solution. The National Archives of Norway is in close contact with Swedish authorities and follows the Swedish eARDproject (e-Archive and e-Diarium) with interest.

Conclusion

Norway's approach to open government information is achieved through a well-defined and well-integrated framework of controls that are among the most advanced in the world. Its long term commitment to building a framework of laws, functional requirements, and technical systems for making reliable government information available to everyone, has enabled a remarkable degree of openness that directly benefits citizens by ay enabling them to know what their government is doing and spending. The consistent application of well-defined Noark requirements has generated a common set of metadata that makes it possible to trace, relate, and compare policies, decisions, actions, and expenditure accurately over long periods of time as a basis for an informed and socially just society.

In the future, the availability of metadata and linked records will be an enormous advantage to the public and the private sector, so long as trustworthy information can be extracted automatically and made available through a platform such as the OEP, a digital repository or an open data or open government platform. Norway is in the process of finding a new balance between carefully defined requirements for managing information and the need to use technology to streamline information management functions.

While specific to Norway, the essence of the systems that have been developed and are being developed could be examined and modified for use internationally and scaled to existing resources, for example to meet lower resource country requirements and financial constraints, especially as Norway's systems are all open source. In this way, Norway's potential contribution to the open government process is enormous.

Notes

1. http://www.constitution.org/cons/norway/dok-bn.html.
2. Case documents of an administrative agency are those that have been received by or submitted to the agency or which the agency itself has drawn up in relation to that agency's area of responsibility or activities.
3. The Directorate later evolved into the Agency for Public Management and eGovernment (Difi).
4. The National Archives of Norway developed ADDML in collaboration with the National Archives of Sweden in 1998.
5. http://public.ccsds.org/publications/archive/650x0m2.pdf.
6. http://www.iso16363.org/standards/iso-16363/.
7. https://www.oep.no/?lang=en.
8. Case handling is the work process involved in handling a request, an enquiry, or an application in order to make a decision or give an answer.
9. https://www.youtube.com/watch?v=HCh3UnDqa3k.
10. http://presse.no/offentlighet/.
11. http://www.opengovguide.com/country-examples/norway-has-developed-an-electronic-public-records-tool-which-is-used-by-central-government-agencies-to-publicise-their-public-records-online-and-which-is-open-for-everyone-to-use/.
12. SAMDOK: Digital Created Material in the Municipal Sector (1985 to 2010), 2015.
13. SAMDOK Report and N4OK: Kvalitetsvurdering av Avletvert Materiale (in English), http://www.kdrs.no/sites/default/files/filer/Tor%20Eivind%20Johansen/n4ok_rapport.pdf, 2014
14. eArchive in Public Administration: Establishing a Data-Driven Infrastructure for Ongoing Transfer of Electronic Records to eArchive and Digital Repository, an Economic Analysis, Commissioned by the National Archives, 2015.
15. The SAMDOK report quoted a 2014 survey of digitally created content in the 428 municipalities and 19 counties. Of the records created in the period 1985 and 2010 in 12,000 case-filing systems and business systems, records from only 1000 systems were secured in custody.

List of Relevant International Standards

Records Management/Information Governance and Risk Related Standards

GENERALLY ACCEPTED RECORD-KEEPING PRINCIPLES

The Principles provide a high level overview of the principles of information governance. Developed by ARMA International to foster awareness of information governance standards and principles and to assist organizations in developing information management systems with which records and information assets are expected to comply. The Principles set forth the characteristics of an effective information governance program but allow flexibility based upon the unique circumstances of an organization's size, sophistication, legal environment, and resources.

Principle of Accountability

A senior executive (or a person of comparable authority) shall oversee the information governance program and delegate responsibility for records and information management to appropriate individuals. The organization adopts policies and procedures to guide personnel and ensure that the program can be audited.

Principle of Integrity

An information governance program shall be constructed so the information generated by or managed for the organization has a reasonable and suitable guarantee of authenticity and reliability.

Principle of Protection

An information governance program shall be constructed to ensure a reasonable level of protection for records and information that are private, confidential, privileged, secret, classified, or essential to business continuity or that otherwise require protection.

Principle of Compliance

An information governance program should be constructed to comply with applicable laws and other binding authorities, as well as with the organization's policies.

Principle of Availability

An organization shall maintain records and information in a manner that ensures timely, efficient, and accurate retrieval of needed information.

Principle of Retention

An organization shall maintain its records and information for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements.

Principle of Disposition

An organization shall provide secure and appropriate disposition for records and information that are no longer required to be maintained by applicable laws and the organization's policies.

Principle of Transparency

An organization's business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate interested parties.

NOARK 4
NORWEGIAN RECORDKEEPING SYSTEM—VERSION 4

Noark-4 is a specification of functional requirements for electronic recordkeeping systems used in public administration in Norway. The specification lists requirements with regard to information content (what kind of information it should be possible to register and retrieve), data structure (design of each data element and the relationship between these elements), and functionality (the functions which the systems are to maintain). In some cases there are requirements with regard to the user interface (how the systems communicate with the users), but this is mainly left to the individual system developers or vendors to decide. The specification does not contain requirements with regard to the how the data structure is to be implemented, or with regard to system design. This is left to the system developers.

NOARK 5
STANDARD FOR RECORDS MANAGEMENT

Noark 5 sets out requirements concerning record structure, metadata and functionality, but does not contain any requirements concerning how these requirements should actually be met in system development. Noark 5 therefore does not define a system, but facilitates different solutions. The requirements are stricter for depositing, transfer and migration. Obligatory metadata must be included in the export, and the export must have a defined structure. The standard does not contain a description of procedures or the way in which different requirements can be met.

ISO 14721
SPACE DATA AND INFORMATION TRANSFER SYSTEMS—OPEN ARCHIVAL INFORMATION SYSTEM (OAIS)—REFERENCE MODEL

The standard establishes a common framework of terms and concepts that make up an Open Archival Information System (OAIS). It allows existing and future archives to meaningfully compared and contrasted. It provides a basis for further standardization within an archival context and it should promote greater vendor awareness of, and support of, archival requirements. An OAIS is an archive that has accepted the responsibility to preserve information and make it available for a designated community. The information being maintained has been deemed to need long-term preservation, even if the OAIS itself is not permanent. Long term is long enough to be concerned with the impacts of changing technologies, including support for new media and data formats, or with a changing user community. Long Term may extend indefinitely. In this reference model there is a particular focus on digital information, both as the primary forms of information held and as supporting information for both digitally and physically archived materials.

ISO 15489:2001
RECORDS MANAGEMENT

ISO 15489 is the foundation standard which codifies best practice for records management operations.

ISO 15489 Part 1: General gives a high level framework for record-keeping and explains the benefits of good records management, the legal considerations and the importance of making someone responsible for recordkeeping. This part also looks at what's needed for good records management, designing recordkeeping systems, records management processes, auditing and training.

ISO 15489 Part 2: Guidelines is a guide to putting the advice given in Part 1 into practice. It provides specific detail on developing records management policy and responsibility statements and suggests a process for developing recordkeeping systems. It also provides advice about developing records processes and controls. It also gives specific advice about setting up monitoring, auditing, and training programmes.

ISO 16175-1:2010 INFORMATION AND DOCUMENTATION—PRINCIPLES AND FUNCTIONAL REQUIREMENTS FOR RECORDS IN ELECTRONIC OFFICE ENVIRONMENTS—PART 1: OVERVIEW AND STATEMENT OF PRINCIPLES

ISO 16175-1 establishes fundamental principles and functional requirements for software used to create and manage digital records in office environments. It is intended to be used in conjunction with ISO 16175-2 and ISO 16175-3. ISO 16175-1 establishes the principles of good practice, guiding principles, implementation guidelines, and it lists risks and mitigations for the purposes including: enabling better management of records in organisations, supporting the business needs of an organisation by enabling greater effectiveness and efficiency of the operations; providing enhanced abilities to support auditing activities; improving capabilities to comply with statutory mandates specified in various information-related legislation (for example, data protection and privacy); supporting good governance (for example, accountability, transparency and enhanced service delivery) through good management of records; and maximizing cross-jurisdictional consistency regarding the articulation of functional requirements for managing records.

ISO 16175-2:2011 INFORMATION AND DOCUMENTATION—PRINCIPLES AND FUNCTIONAL REQUIREMENTS FOR RECORDS IN ELECTRONIC OFFICE ENVIRONMENTS—PART 2: GUIDELINES AND FUNCTIONAL REQUIREMENTS FOR DIGITAL RECORDS MANAGEMENT SYSTEMS

ISO 16175-2:2011 articulates a set of functional requirements for digital records management systems. These requirements apply to records irrespective of the media in which they were created and/or stored. It is applicable to products that are often termed 'electronic records management systems' or 'enterprise content management systems'. ISO 16175-2:2011 uses the term digital records management systems for those software applications whose primary function is records management. It does not seek to set requirements for records still in use and held within business systems. Digital objects created by email, word processing, spreadsheet and imaging applications (such as text documents, and still or moving images), where they are identified to be of business value, are managed within digital records management systems which meet the functional requirements established in ISO 16175-2:2011.

Records managed by a digital records management system can be stored on a variety of different media formats, and can be managed in hybrid record aggregations that include both digital and non-digital elements. ISO 16175-2:2011 does not give specifications for the long-term preservation of digital records; this issue needs to be addressed separately within a dedicated framework for digital preservation or 'digital archiving' at the strategic level. These digital preservation considerations transcend the life of systems and are system independent; they need to be assessed in a specific migration and conversion plan at the tactical level. However, recognition of the need to maintain records for as long as they are required is addressed in ISO 16175-2:2011, and potential format obsolescence issues need to be considered when applying the functional requirements.

ISO 16175-3:2010
INFORMATION AND DOCUMENTATION—PRINCIPLES AND FUNCTIONAL REQUIREMENTS FOR RECORDS IN ELECTRONIC OFFICE ENVIRONMENTS—PART 3: GUIDELINES AND FUNCTIONAL REQUIREMENTS FOR RECORDS IN BUSINESS SYSTEMS

ISO 16175-3:2010 specifies general requirements and guidelines for records management and gives guidelines for the appropriate identification and management of evidence (records) of business activities transacted through business systems. It provides guidelines to assist in: understanding processes and requirements for identifying and managing records in business systems; develop requirements for functionality for records to be included in a design specification when building, upgrading or purchasing business system software; evaluating the records management capability of proposed customized or commercial off-the-shelf business system software; and reviewing the functionality for records or assess compliance of existing business systems.

ISO 16175-3:2010 specifies requirements for export supports preservation by allowing the export of records to a system that is capable of long-term preservation activities, or for the ongoing migration of records into new systems. It does not specify requirements for the long-term preservation of digital records, and it is not applicable to records management in highly integrated software environments based on service-oriented architectures.

ISO 16363:2012:
SPACE DATA AND INFORMATION TRANSFER SYSTEMS—AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

This standard is for use as the basis for providing audit and certification of the trustworthiness of digital repositories. It provides a detailed specification of criteria by which digital repositories shall be audited. This document is meant primarily for those responsible for auditing digital repositories and also for those who work in or are responsible for digital repositories seeking objective measurement of the trustworthiness of their repository. Some institutions may also choose to use these metrics during a design or redesign process for their digital repository.

ISO 23081
INFORMATION AND DOCUMENTATION—RECORDS MANAGEMENT PROCESSES—METADATA FOR RECORDS

Part 1: Principles

ISO 23081 sets a framework for creating, managing and using records management metadata and explains the principles that govern them. It is a guide to understanding, implementing, and using metadata within the framework of ISO 15489. It addresses the relevance of records management metadata in business processes and the different roles and types of metadata that support business and records management processes. It also sets a framework for managing those metadata. It assesses the main existing metadata sets in line with the requirements of ISO 15489.

Part 2: Conceptual and implementation issues

This part of ISO 23081 focuses on the framework for defining metadata elements for managing records and provides a generic statement of metadata elements, whether these are physical, analogue, or digital, consistent with the principles of ISO 23081-1.

ISO 26122 INFORMATION AND DOCUMENTATION—WORK PROCESS ANALYSIS FOR RECORDS

This standard provides guidance on work process analysis from the perspective of the creation, capture and control of records. It identifies two types of analyses, namely functional analysis (decomposition of functions into processes), and sequential analysis (investigation of the flow of transactions). Each analysis entails a preliminary review of context (i.e., mandate and regulatory environment) appropriate for the analysis. The components of the analysis can be undertaken in various combinations and in a different order from that described here, depending on the nature of the task, the scale of the project, and the purpose of the analysis. Guidance provided in the form of lists of questions/matters to be considered under each element of the analysis is also included.

The standard describes a practical application of the theory outlined in ISO 15489. As such, it is independent of technology (i.e., can be applied regardless of the technological environment), although it can be used to assess the adequacy of technical tools that support an organization's work processes.

ISO/IEC 27001:2013 INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—INFORMATION SECURITY MANAGEMENT SYSTEMS—REQUIREMENTS

This standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. This standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The standard covers information security leadership and high-level support for policy, planning an information security management system; risk assessment; risk treatment, supporting an information security management system, making an information security management system operational, reviewing the system's performance, and corrective action.

ISO 30300:2011
INFORMATION AND DOCUMENTATION—MANAGEMENT SYSTEMS FOR RECORDS—FUNDAMENTALS AND VOCABULARY

This standard defines terms and definitions applicable to the standards on management systems for records (MSR) prepared by ISO/TC 46/SC 11. It also establishes the objectives for using a MSR, provides principles for a MSR, describes a process approach and specifies roles for senior management. It is applicable to any type of organization that wishes to establish, implement, maintain and improve a MSR to support its business; assure itself of conformity with its stated records policy; and demonstrate conformity with this standard by undertaking a self-assessment and self-declaration. It also supports organizations seeking confirmation of its self-declaration by a party external to the organization, or seeking certification of its MSR by an external party.

ISO 31000: 2012
RISK MANAGEMENT—PRINCIPLES AND GUIDELINES

The standard provides principles, a framework, and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment. However, ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programmes. Organizations using it can compare their risk management practices with an internationally recognised benchmark, providing sound principles for effective management and corporate governance.

Data Management Standards

DATA QUALITY ASSESSMENT FRAMEWORK (DQAF)

The International Monetary DQAF[1] provides a structure for assessing countries' data quality against a structure of internationally accepted practices and methodologies. It covers institutional environments, statistical processes, and characteristics of the statistical products. It is organized around a set of prerequisites and five dimensions of data quality: integrity, methodological soundness, accuracy and reliability, serviceability, and accessibility. It identifies quality-related features of governance of statistical systems, statistical processes, and statistical products. It is rooted in the UN Fundamental Principles of Official Statistics and incorporated good practices developed by the IMF's initiatives on data dissemination: the Special Data Dissemination Standard (SDDS) and the General Data Dissemination System (GDDS).

DATA DOCUMENTATION INITIATIVE (DDI)

The DDI is a quality assessment framework developed as an international standard for describing data from the social, behavioral, and economic sciences. It aims to address obstacles to creating good structured It provides a metadata specification expressed in XML. The DDI project, which started in 1995, has steadily gained momentum and evolved to meet the needs of the social science research community including universities, data archives, research centers and institutes, and data services. The metadata specification now supports the documentation and integration of entire research data lifecycle. DDI metadata accompanies and enables data conceptualization, collection, processing, distribution, discovery, analysis, repurposing, and archiving in relation to the organizational needs of the creators and the data being described.

Note

http://dsbb.imf.org/Pages/DQRS/DQAF.aspx.


WORLD BANK GROUP