Tidsskriftet Arkiv

VOLUM 8-2 2017

DOI: http://dx.doi.org/10.7577/ta. 2485
ISSN 1891-8107

FAGARTIKKEL

Olav Hagen Sataslåtten

The Norwegian Noark Model Requirements for EDRMS in the context of open government and access to governmental information

Introduction

This article analyses the relationship between the Norwegian Noark Standard and the concepts of Open Government and Freedom of Information. Noark is the Norwegian model requirements for Electronic Documents and Records Management Systems (EDRMS). It was introduced in 1984, making it not only the world's first model requirement for EDRMS, but also, through the introduction of versions from Noark 1 to the present Noark 5, internationally the model requirement with the longest continuation of implementation.

In accordance with the 2008 revised Norwegian Freedom of Information Act, the Norwegian authorities in May 2010 launched an updated Electronic Public Records system, or (Offentlig Elektronisk Postjournal or OEP) (Norway https://www.oep.no/?lang=en). OEP is a web-based portal in which central governmental agencies are required to regularly publish their newly registered electronic metadata records. It is metadata registered in the Noark systems within governmental bodies which is made available in the OEP system.

In order to better understand the technical outline and functionality of the Noark model requirements, it is necessary to see the connection to the wider framework of the Norwegian governance legislation and its Freedom of Information (FOI) Act (Norway, *Freedom of Information Act*, 2006) on the right of access to documents held by the public administration and public undertakings. Freedom of Information is the foundation on which the Norwegian Open Government platform (OEP) rests, as it aims to increase openness and transparency in the Norwegian society. Being one of the first national initiatives to incorporate in a single platform an up-to-date nationwide registry of metadata deriving from the EDRMS of the governmental sector, OEP is a model which could have relevance in open government settings also outside of Norway.

From a juridical point of view, the Noark standard was not created in a vacuum. Noark would unlikely be designed in the same way back in 1984 if the Norwegian Public Administration Act and the Norwegian FOI Act had not been introduced in 1967 and 1970 respectively. The direct relation between those two acts and Noark is expressed through the manner in which Noark fuses and secures principles of governance, transparency and predictability into its own core. This is accomplished through a fixed set of functional requirements defined as mandatory in the model.

The mandatory requirements in Noark have increased in number from the introduction of Noark 1 in 1984 to the launch of Noark 5.2 in 2012. The increase in complexity is a direct result of the general increase in the digitization of our society, establishing fully electronic communication channels between governmental bodies as well as between them and the public at large. Successively, the mode of interaction, to an increasing degree interlinked, between governmental organisations, cross-sector and regions, generated a need to develop the Noark standard within a framework of big data and integration.

The requirements which made OEP possible were already in place in 1993 with the launching of Noark 3, since a web-based platform, The Electronic Records Registry (See Difi http://www.difi.no/artikkel/2009/11/elektronisk-postjournal-epj), EPJ in Norwegian, similar to the OEP had already been launched. The EPJ registry covered all ministries and made the metadata of the governmental public records available online to approximately 140 subscribing newspapers and television agencies. It was undoubtedly the success of the EPJ Electronic Records Registry that lay the foundation for the OEP Public Electronic Records platform launched in 2009. The EPJ was not mandatory through the FOI Act, but its success led to the creation of the OEP requirements introduced in the new FOI Act in 2009.
All public records in Norway are accessible to the public unless subject to a few clauses in the FOI Act. The Act does not allow governmental organisations to withhold a full record. It can only withhold certain passages in a record that fall under one of the few clauses that limits access to the information. This undoubtedly makes Norway one of the most open countries in the world in terms of access to information, since The Archives Act (Norway. *The Archives Act,* 1992) puts a requirement on all public organisations to register all incoming, outgoing and internal

documents in Noark if they generate case handling activity in the organisation, or serves as documentation for the same. The linking of the law with a technical solution like the OEP under the auspices of a very far-reaching FOI Act makes the scenario of openness real and concrete, and not just a grand vision of the future.

Today the OEP service includes more than 1000 governmental agencies. Norway separates state sector and municipal sector and, as of present, the municipal sector with its 428 municipalities is not required to provide its metadata from its Noark systems to the OEP platform. The majority of Norwegian municipalities have nevertheless established their own solutions, making their metadata public on their own websites normally 2-3 days after its registering in the agencies.

An overview of the public's use of the OEP

The most common search terms used by the public in the OEP platform are: report, complaint, inspection, demand, revision, supervision, deviation, work accident, incident, evaluation, illegal, serious and allotment letter.

Figure 1 provides an excerpt of statistics which indicate of the number of requests for records per agency in March 2014, and hence the extent of demand. Comparing the number of requests with the number of published documents (Figure 2), one may observe that for instance the Ministry of Justice received 28687 orders, but chose to publish nearly 52212. The figure is perhaps even more surprising when comparing the number of requests sent to the Norwegian Labour Inspection Authority, which received a total of 44993 requests, and published almost four times the amount - 160061.

Agency	Number of orders
Norwegian Labour Inspection Authority	44993
Ministry of Justice and public security	28687
Ministry of Foreign Affairs	24238
Ministry of Culture	20786
Ministry of Petroleum and Energy	17685
Ministry of Health and Care Services	17255
Ministry of Transport and Communications	15102
Ministry of Climate and Environment	15042
Norwegian Water Resources and Energy Directorate	14845
Climate and Pollution Agency	14343
County Governor in Troms	13030
National Police Directorate, Norway	12970
County Governor of Hordaland	12866
County Governor of Oslo and Akershus	12786
Ministry of Education and Research	12366
County Governor of Sogn og Fjordane	11577
County Governor of Nordland	11209
Directorate of Fisheries	11187
Ministry of Government Administration, Reform and Church Affairs	10942
Civil Aviation Authority Norway	10472
Ministry of Children, Equality and Social Inclusion	10100
Ministry of Fisheries and Coastal Affairs	9493
County Governor of Vestfold	9485
Ministry of Finance	9426
Financial Supervisory Authority of Norway	9341
Ministry of Defence	9322
Norwegian Directorate of Health	9056
Directorate for Civil Protection and Emergency Planning	8826
Ministry of Trade and Industry	8771

Figure 1 Number of requests for records per agency in March 2014

Agency	**Number of documents**
Norwegian Labour Inspection Authority	160061
The Road Authority Region East	147832
Norwegian State Housing Bank	128524
The Road Authority Region South	111130
The Road Authority Region West	109600
The Research Council of Norway	102411
Norwegian Directorate of Health	84249
Norwegian Gaming and Foundation Authority	83392
National Archives of Norway	78890
Directorate of Fisheries	77092
The Road Authority Region Centre	74698
Norwegian Medicines Agency	68307
Ministry of Foreign Affairs	66654
The Road Authority Region North	62125
Norwegian Maritime Directorate	60344
Norwegian Agency for Development Cooperation	59472
Directorate for Civil Protection and Emergency Planning	55937
Norwegian Directorate for Education and Training	54682
County Governor of Oslo and Akershus	52540
Ministry of Justice and public security	52212

Figure 2. Total number of published documents per agency in March 2014

The framework of metadata submission from the Noark systems to the OEP

We should bear in mind that the submission of metadata onto either the EPJ or the OEP never was and is still not performed from a digital repository as such. The storage of data and electronic documents in the governmental bodies is not in any way subject to the technical framework or the international standards governing what is commonly understood as a trusted digital repository. The trust factor, as this article aims to demonstrate, lies elsewhere.

From the mid 1990s until present, the submission of metadata from agencies, first to the EPJ and later to the OEP, is performed daily from each governmental agency through the standardised report generators included in the Noark systems. The EPJ solution was handled by the State's Governance Service as from 1993, and the OEP from its launching in 2010 by the Directorate for Governance and ICT (DIFI).

The metadata structure

In order to grasp the context in which the OEP platform is based, it is necessary to analyse two vital aspects. The first is a fixed set of metadata and the second is the fixed manner in which these metadata are structured. Noark was not mandatory for the governmental sector until 1999, but it was the *de facto* standard for EDRMS for all governmental bodies as from its launching in 1984. Simultaneously, with the introduction of the Noark standard, the National Archives in 1984 introduced guidelines for the *Implementation of Computerized Registering Systems in the Governmental Sector*, and *Instructions for Records Management in the Governmental Sector (See Noark 1, p67).* It was the Governmental Rationalisation Directorate that was responsible for the Noark standard until1990, when the responsibility was transferred to The National Archives.

By 1990 more than 90 governmental institutions were using Noark-systems, including all ministries. The Noark systems were perceived as having better functionality, stability and features than any other records and document systems at the time of its launching. Henceforth, the EDRMS of the public sector in Norway as of 1984 was to a large extent a homogeneous entity, all compliant to the requirements outlined in Noark. The consistency of such a regime facilitated a standardised approach to how the metadata from the systems could be made available to the public. There were no unknown factors, no unpredictability and no governmental body not complying with the model. In this way, the central agency governing the OEP predecessor could already from the mid 1980s order a standardized set of metadata delivered from all central government agencies. These sets were uploaded to the web based platform, if not on a daily basis at least twice or three times weekly.

The mandatory metadata requirements of Noark had already been introduced through Noark 1 in 1984. In 1970, Norway introduced archives regulations for the central governmental agencies, regulations which in actuality bore legislative impact. These regulations were mirroring principles formed within the Public Administration Act of 1967 (Norway. *Public Administration Act* 1967) and the Freedom of Information Act of 1970 (Norway. *Freedom of Information Act* 1970). They first and foremost addressed the need to be able to identify documents and the metadata related to them in a manner which secured predictability, consistency, traceability and search ability. There were eight metadata elements which were re-instated in the Archives Act of 1992 (presented to the Parliament in 1992 but not launched until 1999). These metadata are comprised of a concentrated amalgam of the following information elements:

a) date of registration
b) record, file and document number
c) sender or recipient information
d) information describing record, content or subject
e) document date
f) classification code

g) date or method in which an enquiry has been processed or preparation of a letter or cover note has been completed.

The concept of authenticity versus the issue of context and integrity

Noark puts very strict conditions for the fixity and automatic parameter setting of records creation, already in Noark 1 in 1984. With the introduction of a project in 2009 within The National Archives of Norway for the implementation of a repository system for the preservation of electronic records, issues related to authenticity emerged. The extraction of metadata and electronic documents from the EDRMS of governmental agencies, together with the actual transferal of the same to The National Archives, raised some fundamental issues related to trust and authenticity. The discussion circled around core concepts such as "If a trusted digital repository is indeed to carry trustworthiness to the public, where lies the mechanisms actually securing trust?" Was it possible to pinpoint the motions securing authenticity, thereby making the statement "What we store in our National Archives is indeed authentic material, identical to what was once produced in the governmental agencies." Is it possible to secure authenticity of electronic records produced in governmental agencies? Is the issue relevant at all? Is authenticity the crucial factor, or is *integrity* the concept we should focus on? Is not the combination of *context* and *integrity* more vital than that of authenticity? Is it not of fundamental importance for a digital repository to be able to demonstrate that what it stores upholds the *contextual authenticity* of the electronic records rather than focusing on the notion of "This is the original"? [1]

The framework of the contextual authenticity of records is more vital than that of the authenticity of each individual digital object. This is so because an EDRMS combines both metadata structures and digital objects. The metadata structure, if produced in a system compliant with the Noark model requirements, carries with it information related to "why, when, how and by whom?" These are aspects fundamental for the ability to demonstrate authenticity. This is a framework of context and integrity rather than the issue of demonstrating the idea of "the original document". It is necessary to step away from the concept of the storing of original records or documents in an electronic setting, since authenticity cannot rest on such a notion. The ability to demonstrate that what is stored in the repository carries the same structure as what was produced in the governmental agencies is the fundamental issue.

Metadata within the Noark systems

The record number metadata was automatically generated by the system and programmed on the basis of the duration of a year. As a result, all records created within the year 1984 would follow

[1] The issue of authenticity in electronic records is analysed in depth by the Interpares Project through their Authenticity Task Force Report. See http://www.interpares.org/book/interpares_book_d_part1.pdf accessed 1 Sep 2014.

a fixed parameter, starting as 84/0001 and successively rising with each record created, potentially ending with, for instance, the record number 84/1725 within the timeframe of the year 1984.

The following parameters were fixed in Noark 1 of 1984, and the recording of the information was a mandatory requirement. As may be observed, they reflect the core of the metadata described earlier:

a) classification code
b) record number
c) record creation date
d) classification
e) name of department creating the record
f) name of employee responsible for the institutional activity documented in the record
g) precedence
h) retention code
i) cross reference to other records
j) description of subject matter
k) number of documents in the record
l) date of last document in the record
m) initials of employee presently keeping the record if physically brought out of the archives.

Consistent and fixed electronic records management on a national level over a time span of 30 years

The Noark standard is undoubtedly rigid. To what extent such a model requirement could be introduced as mandatory for governmental agencies in for instance the EU is a question which to some extent was answered during the Digital Roadmap conference arranged by UNESCO, the ICA and IFLA in The Hague on the 5th of December 2013. In that meeting, a representative from the EU Commission was asked if not a firmer approach to mandatory requirements for electronic records and digital preservation could be introduced in the EU, upon which he stated the Commission's reluctance to introduce even more mandatory requirements in this field. Not only is the Noark standard rigid, the legislative framework surrounding it, particularly the one making it mandatory for all governmental agencies to implement Noark, may be perceived as both static and inflexible. On the other hand, in Norway, standardization has facilitated a common set of metadata with a fixed structure which is traceable 30 years back in time. Automatic metadata extractions are henceforth possible to accommodate, both to a platform such as the OEP, a digital repository or an open data or open government platform.

Noark viewed retrospectively

In order to discuss the development of metadata requirements in Noark, it is necessary to consider that the development of the standard to a large degree happened in line with the development of new technologies, new modes of interaction across sectors, and a rapid digitalization of society.

Noark 1

A very significant part of Norwegian records management regulations since long before the introduction of Noark, is the function of signing off a record. Signing off a record is performed when the issue to which the records relates has been solved or dealt with, either through the creation of an outgoing document, or the case handler marking off on the record that the matter has been dealt with. This function undoubtedly has facilitated a broader framework of transparency and accountability in the Norwegian public sector, since the generating of reports, most often on a monthly basis, showing which records have not been handled, creates an overview for the executive level on which it may act to prioritise the solving of the issues to which the records relates. This function is part of the original metadata requirements of Noark and has been a constant all the way from Noark 1 to Noark 5, firmly established in Norway's Archives Act and all regulations established prior to this. Because all metadata parameters in a Noark system are searchable in an advance search mode, a search in the signing off-parameter might serve as an excellent tool for generating statistics of how many records are pending decisions.

From Noark 1 to Noark 2

With Noark 2, introduced in 1987, the following new functions were implemented:

> a) Functionality for the registering of internal cover notes and note verbal in order to be able to create a wider and more comprehensive backdrop for the case handling.
> b) Department-based registering functions in order to eliminate the risks of duplicate records, as well as creating reports and overviews showing the transferral of records from department to department.
> c) Functionality for access control to specific records.

Noark 3

With Noark 3 of 1994, the classification system (codes) was introduced based on the Common Classification System of The State Administration of 1988. The importance of classification codes in Noark has not decreased, seeing a further accentuating of its principles with the introduction of Noark 5 in 2008, and increasingly strengthened as a structural component in Noark 5 v 3.1 introduced in 2013.

Noark 3 to Noark-4

From Noark 3 to Noark 4, the latter implemented in 1999, the most crucial changes were made in order to facilitate the introduction of digitized documents as well as e-mails.

The trust factor

To what extent is transparency and openness embedded in the combination of these mandatory registration requirements? A whole nation of lawyers, patients, victims, journalists, common people and Members of Parliament takes the accuracy and validity of the metadata transported from these records and into the OEP for granted. Perhaps is it so that, since the FOI Act guarantees access to all public records (with the exception of classified files), the validation of content through the citizen's right of access in itself safeguards authenticity through each and everyone's potential examination of the contents of the records? Any citizen may order hardcopies, and in that function there are potentially as many watchdogs as there are people capable of ordering and reading records.

Would Noark have any purpose in a country lacking freedom of information? Could Noark function without appropriate Governance Acts? Noark is tailored according to the principles of good governance established by the Public Administration Act and its related laws and regulations. The governance is transparent due to FOI Act which actually guarantees every citizen's access to information which may be traced via an open government portal. Noark is merely the tool through which all this is accomplished. The Noark system did not create itself – it was created as a means to secure the fundaments of accountability and openness the State initially and continuously guarantees the public.

In Noark 3 (1994), introduced in 1994, the close relationship between the legislative areas of governance and freedom of information was accentuated, directly expressed through the following paragraphs from the introduction:

> It is necessary to highlight the close relationship between governance and legislation. Case handling follows written guidelines, and is based on principles of precedence and common practise. The decisions may be bound by precedence or be creating precedence, as in court practise. Cases that are similar in nature require similar decisions. Accordingly, the demands placed on the governmental body's own records administration increases. The practise of written case handling has resulted in a significant increase in the number of records in the governmental sector. In addition, the cases very often require extensive case handling time. They may run in the system for numerous years, and the number of documents rises. A significant number of documents thereby have to remain active. They have to be registered, joined together in a logical sequence and correlation, and they have to be quickly retrieved over a significant time span <….>. The legislation pertaining to freedom of information has put demands on the registering practice. The decision which maintains the individuals or the public's rights towards the public sector are brought into focus as the central aspects of the registration of records, and has made it more significant. The new legislation has simultaneously increased the complexity of the registration procedures, making them more demanding.

The trust factor and OEP

An adequate analysis describing the principles of trust embedded in the weekly or daily dissemination of metadata from the Noark databases to the OEP somehow has to explain certain parameters. These parameters within the Noark requirements eliminate the possibility of unauthorised deletion, alteration or manipulation of metadata and documents in the databases of the governmental organisations. The combination of parameters also creates context. The metadata transferred from the Noark systems to the OEP platform may never have been stored within a trusted digital repository. Transfer to the OEP happens weekly, whilst transfer to the repository of The National Archives is performed far less seldom –perhaps every 10th year. The contents of the Noark-based systems are not stored in trusted digital repositories in the governmental agencies, but remain part of the ordinary grid of servers and databases.

The OEP Public Electronic Records platform is not related to a digital repository in terms of integration. A digital repository is a complex framework of digital preservation lifecycle management operations. The way metadata is being transported from the individual databases underlying the EDRMS of each public agency into the OEP Public Electronic Records platform is, by comparison, very simple. Each EDRMS has a report generating function, where the metadata registered within a selected timeframe is being saved in a file. The content of this file is then distributed into the OEP database. The ability to create such a report has been mandatory in Noark since the first edition in 1984. What distinguishes these types of reports from other kinds of Noark system generated reports is the very detailed "rights grid" implemented in Noark. The system allows each record to be tagged in a manner which prohibits the publication of certain metadata elements which fall under the categories restricted from publication by the FOI Act. Noark requires the function "Exempt from publication" as an option for each individual record.

Noark-4 as framework for the Public Electronic Records (OEP) platform

With Noark 4, introduced in 1999, radical shifts in the approach to requirements were implemented. Noark 4 is divided in two parts, the first being functional requirements, the second technical. Consisting of 235 and 254 pages respectively for functional and technical requirements, it is a version of the standard which in terms of complexity never has seen a complete implementation. Particularly because of its inclusion of technical specifications for sector-based integration of EDRMS, those aspects were somehow premature at such an early stage as 1999. Noark-4, despite its overtly complex structure, provided the foundation for the OEP platform of Norway. This article provides the first ever English translation of the mandatory requirements of Noark-4. The translation is deemed crucial for the understanding of what was in place in Norway of mandatory metadata requirements since 1999, making the OEP functionality possible.

The Noark-4 mandatory requirements

In order for a Noark-4 solution to be accepted in a governmental agency it needed to fulfil the following requirements:

Requirement K3.13: All information registered or altered needs to be immediately available for other functions or other users.
Requirement K3.14: It shall not be possible to perform registrations or alterations conflicting with the rules appearing from the technical description.
Requirement K3.15: For parameters where in the table description a reference to a supplementing register is noted, it must be possible to gather an overview of valid values from this supplementing registry, following the criteria stated in the technical description.
Requirement K3.16: For supplementing registries where the number of values may be large, it should be possible for the user to search for the correct value on the background of information stated in the supplementing registry and eventually other tables carrying a relation to this.
Requirement K3.17: For parameters where it is stated in the table description a reference to another supplementing registry, it shall not be possible to register values not present in the supplementing registry, unless it explicitly stated in the technical description that this is valid.
Requirement K3.18: By the registering of new records, the system shall where it is possible show the parameters in the registering mode fully given with standard values, gathered from the context in which the registering happens and in the role of the user. As a minimum the standard values under the individual attributes given in the technical description is to be used.
Requirement K3.20: All dates/points in time are to be registered with 4 digits for one year. The same applies to years included in the record number and reference number and so forth, irrespective of two or four digits appears in the presentation view.

3.3.3 Search requirements
Requirement K3.21: All attributes with a limited length (that is, not undefined search parameters or binary parameters) in all parameters are to be searchable.
Requirement K3.22: Information stated as diverted attributes are to be searchable identically with all other attributes.
Requirement K3.23: In every search, capital all small letters are to be treated as equivalents.
Requirement K3.24: In a search it shall be possible to state values for several parameters in the same table and with the "AND" function between the fields.
Requirement K3.25: In a search, it should be possible to state "OR" functions between fields or groups of fields.
Requirement K3.26: For all date fields and numerical fields it must be possible to search on an interval of values.
Requirement K3.27: For text fields with a limited length, it must be possible to state left or right truncation in search mode.
Requirement K3.28: Where it falls natural, it shall be possible to search in information from several tables simultaneously. This in particular is related to the tables Case, Classification, Part in the Case, Record, Sender/Receiver and Record Description.
Requirement K3.32: The user is to be presented information on how many hits stemming from a search.
Requirement K3.42: Any search is to be limited to the rights given by the user's roles, authorization for access codes or membership in access groups.

3.3.4 Requirements for technical design
Requirement K3.43: The system is to handle the transfer to the year 2000 without the need for any manual operations.

Requirement K3.44: The system is to facilitate the standardized use of security backups. Description of routines for security backups are to be included as part of the system documentation.
Requirement K3.45: The system is to have recovery functions so that the information integrity is maintained at interferences such as power cups or hardware failure.
Requirement K3.46: It shall not be possible to delete records referred to from other tables.
Requirement K3.47: It shall not be possible to alter key attributes used when referring from records in other tables, without the equivalent attributes are altered in the record referring.
Requirement K3.48: All functions creating updating of more than one record is to be performed in such a manner that either all records are updated or none.
Requirement K3.49: The system is to be secured in such a manner that no one can access information they are not authorised to see if they try to use tools other than the Noark system.

3.3.5 Requirements for supplementing information
Requirement K3.50: If the system contains attributes not specified in Noark-4, it must be possible to export these as additional information, according to the principles described in the table Additional Information.
Requirement K3.51: A Noark-system is not to replace attributes defined in Noark-4 with equivalent or similar data elements under other names or with a different structure. If the system is using other attributes-names than stated in chapter 14, then these, at export, have to be converted to the names Noark-4 specifies, with reference to chapter 15.

The Noark-4 Records Management Module
Requirement K4.1: It must be possible to register a document received or produced in an agency as a record. As a minimum it must be possible to register the information defined as obligatory in the table "record entry".
Requirement K4.2: A record entry is always to be related to a case. To a case it shall always be possible to link one or more record entries.
Requirement K4.3: As common information relating to a file one shall as a minimum be able to register the information obligatory for the table.
Requirement K4.4: The representation in screen images shall clearly show that the information is divided in two levels, one for the case and one for the record entry. It must be able to perform registering on both levels simultaneously.
Requirement K4.5: From the relevant screen images it is to be clearly apparent how many records exists under one particular case, including the contents of one particular record entry.

4.2.2 Identification of case and record entry
Requirement K4.6: A case is identified by its case number. The case number consists of year followed by successive numbers (the case's sequence number) within the year span.
Requirement K4.7: The case number is to be presented to the case manager in the form of aa/#####, where aa is the two last numbers in the year and ##### is the sequence number, presented as up to six numbers, but without prefixed zeroes.
Requirement K4.8: It shall not be possible to delete a registered case, and it shall not be possible to alter the case number.
Requirement K4.9: A record entry is to be clearly identified by its serial number. The serial number consists of year and continuous sequence numbers within a year span.
Requirement K4.11: It shall not be possible to delete a registered record entry, and it shall not be possible to alter the serial number (which is the system's internal identification).
Requirement K4.12: It shall also be possible to identify a record entry by its document number, which is a continuous number within the individual cases.

4.2.3 References and overall structure related to case and record entry

Requirement K4.14: When a case is created, the filling of the attributes and registry management unit and series is to be automatic. The values are to be gathered from the role the user is attached to, with reference to the table Person-Role. It shall be possible for the user to alter these values.

Requirement K4.15: In the basic version of Noark-4, it shall as a minimum for each particular case be possible to perform classification with the help of two order values (classification codes). The classification codes may be subject codes and/or object codes, and it must be possible to range them as primary and secondary codes. The agency shall be free to choose classification following The State's Common Classification System and the municipal K-code system.

Requirement K4.16: In the expanded version of Noark-4, it shall be possible to classify a case with an unlimited number of classification codes – subject codes and /or object codes. It shall be possible to make a ranking of the classification codes (primary, secondary, tertiary etc), but it must also be possible to register classification codes without ranking them. These will then function as references to other subjects or objects which the case relates to.

Requirement K4.17: It shall be possible to relate a case to the administrative structure of the agency by filling in the attributes *case-responsible unit* and *case responsible* (the initials of a person). The system shall only allow values previously registered in the system. If the case responsible initials are valid across administrative units, case-responsible unit is to be automatically filled in simultaneously as the case-responsible's initials are registered.

Requirement K4.18: It shall be possible to join cases in a project, with reference to the attribute *project.* A project is a common category to be used when searching for cases that are related

Requirement K4.19: In the basic version it shall be possible to register reference from one case to another.

Requirement K4.20: In the expanded version it shall be possible to register reference from one case to another or to several other cases, or to one or more single records in a case. For this purpose, the table *Compare case* may be used.

Requirement K4.21: It shall be possible to transfer one or more record from one case to another. The transfer means that the record(s) will be given a new case number. The serial number is not to be changed.

Requirement K4.22: Records that are moved is to be automatically given a new document number as of the first available number in the case to which it is moved. The new document numbers are distributed in rising order according to the order the records had in the case it was transferred from.

Requirement K4.23: Records that are not moved is not to be given a new file number unless a complete renumbering is performed in a case.

Requirement K4.24: It must be possible to transfer all records linked to the one and the same case in one collective operation.

Requirement4.25: It must be possible to perform a renumbering of all the file numbers of the records in a case. The renumbering is always to include all records in the case, and is to be performed in one joint operation. The order in which they are arranged is to follow the rising serial numbers of the records.

Requirement K4.26: If the transfer and/or renumbering affects the references to or from the records involved, the references are to be updated automatically so that the system is consistent after the moving/renumbering.

Requirement K4.27: The system is not to allow the transfer of one record if this is signing off other records which are not transferred. If this is attempted, the user is to be notified of which links are blocking the transfer.

Requirement K4.28: All transferal of renumbering is to happen with the use of a specific set of commands, and solely by authorized personnel according to their rights defined in chapter 8. All transferring and renumbering is to be logged by the system in a transparent manner.

Requirement K4.29: When transferring or renumbering, the user is to get reminders asking them to change the required references on the paper records in the archives.

Records in Noark are related to various types of documents which specify which functions the registered documents have. The values allowed for document type in a record are given in the table Document Type and includes the following:

I	Incoming letter
U	Outgoing letter
N	Internal memo (notes, reports etc.) that requires following up and signing off
X	Internal memo which does not require following up or signing off
S	Case drafts

A short analysis of the Noark-4 mandatory requirements in terms of transparency and accountability

As appears through the mandatory requirements listed above, certain key elements will appear to secure fixity of context and the integrity of records. Once there is fixity of context and integrity, will not traceability and search ability follow? The predefined structure provides a map. In the framework of semantics, we may pose the notion that Noark provides a standardised ontology where disclosure of content in combination with context follows a predictable pattern. This provides a common set of search criteria which forms a grid where all information elements and objects may be retrieved, disclosed, presented and communicated. The strength of Noark will appear most clearly when compared to a setting where there is no standardisation or compliance, though legislation is in place. A comparative analysis of conditions in Norway in terms of EDRMS compliance, and any other country in Europe that has refrained from introducing legislative compliance, would provide grounds for a gap analysis. This analysis would presumably provide the elements that will describe which specific Noark requirements safeguards accountability and transparency. The country lacking these mandatory requirements in their EDRMS would then appear to have a decreased set of criteria for securing accountability and transparency. This reduced set of criteria may then be empirically tested, based on the following hypothesis:

a) Non-fixity and randomness in the registering of metadata decrease the possibility of systematic search and systematic retrieval, since search within records presumably requires a combination of two or more sets of metadata. Context is a crucial component in information retrieval from records, and no records contain only one metadata element.

b) With few exceptions, a record relates to another record, and the relation between the two of them is in itself a set of metadata. If the metadata relating the two records does not follow a standardized format, retrieval possibilities will remain random.

c) The unpredictability following inadequate search results will decrease the credibility and the trust factor which should lie imminent within the information system.

d) The absence of adequate search results will lead to an immediate decrease in the public's perception of the system being valid or relevant as a trusted source of information.

e) If metadata within a governmental agency is known to be subject to non-authorised alterations, deletion on changes, trust in the authenticity and integrity of the information provided from the agency will decrease significantly.

This subsequently decreases predictability in the retrieval of information within the EDRMS. The parameters securing non-alteration of metadata once locked in the Noark-compliant EDRMS, may be measured against the absence of the same in any system being compared.

Conclusion

The context in which digital information is produced, as well as the increasing speed of which we as citizens demand access to information, might determine the way we perceive repositories, preservation and the need to bring it all back in its original form five minutes from now or next year. We also see that the modus operandi of the implementation of international standards and frameworks proves that we may all work together in a unified manner to create the best possible solutions that carry relevance, independent of size, national context or legislation. But in order to get there, we believe that the formative stage of data creation has to be addressed. If the we pose the following question: given model requirements, compliance with them safeguards the creation of certain key elements that we shall preserve, and because they were created in a standardized way, will we know how to standardize both ingest, test, preservation and access, search and retrieval?

In order to raise the focal point from the mere strands of preservation to the practical purpose of providing searchable access, certain elements such as logical coherence in metadata structures, advanced search functionality based upon logical criteria and easy to master user interfaces have to be developed. Would it be logical to conclude that if the metadata structures tagging contextual and content based information to the information objects are standardized, cannot all this information be brought back in the future? If everything is identified, labelled and coherently structured, is there really any end to how broad the range of information retrieval may actually be?

With The National Archives of Norway's introduction of apps for its archival portal and its digital archives in 2011 and 2012 respectively, we actually potentially moved some of the contents out of our digital repository to a platform which is right there in the hands of the public. It is an intriguing image, visualizing digital born material extracted from systems long ago rendered obsolete and no longer existing, transformed via resource descriptor frameworks (RDFs) and xml-based technology, brought back to the public in the most relevant and widely used technologies of smart phones and other mobile devices such as pads and tablets.

References:

Difi - Public Management and eGovernment. *The Electronic Records Registry service*. Applications for access via http://www.difi.no/artikkel/2009/11/elektronisk-postjournal-epj

Noark 1 to 5. (1984-2012). Model requirements for EDRMS. http://www.arkivverket.no/eng/content/view/full/200

Noark 3 (1994). Model requirements for EDRMS. https://www.arkivverket.no/arkivverket/Offentleg-forvalting/Noark/Tidligere-versjoner/Noark-3

Norway. *The Archives Act 1992*. 4 December 1992 No. 126.

Norway. *Freedom of Information Act 2006*. 19 May 2006 No. 16

Norway. *Freedom of Information Act* of 19 Sep 1970 No. 69

Norway. *Public Administration Act 1967*. 10 Feb 1967 No.86. See English translation at http://www.ub.uio.no/ujur/ulovdata/lov-19670210-000-eng.pdf

Norway. Electronic Public Records (Offentlig Elektronisk Postjournal - OEP) system https://www.oep.no/?lang=en