Digitale Archivering in Vlaamse Instellingen en Diensten

DAVID

Archiving e-mail

Filip Boudrez

Sofie Van den Eynde

FACULTEIT RECHTSGELEERDHEID

INTERDISCIPLINAIR CENTRUM VOOR RECHT EN INFORMATICA

TIENSESTRAAT 41

B-3000 LEUVEN

Stadsarchief Stad Antwerpen

Version 1.0

Depot D/2002/9.213/1

Leuven - Antwerp, August 2002

E-mail: david@stad.antwerpen.be

Website DAVID project: http://www.antwerpen.be/david

DAVID is a Flemish Research Project Financed by the Fund for Scientific Research in the Scope of the Max Wildiers Foundation

TABLE OF CONTENTS

INTRODUCTION

During the nineties e-mail has developed itself as a popular technology dramatically changing many aspects of our professional and personal life. Numerous studies have been conducted concerning the legal, social and ethical implications of e-mail and the advantages and disadvantages of this new means of communication. Also governments are more and more being faced with the phenomenon of "electronic mail". Networks and electronic mail play an important role in the development of a better service towards the citizens. In Belgium ambitious e-government projects are being undertaken both on federal and on Flemish level[1]. This is also the case for the other Member States of the European Union. The goal is to use user-friendly portal sites to make communication between citizen and government and among governments take place in a quick and efficient way. These experiments would be unthinkable without electronic mail.

According to the Archive Act that applies to them, government administrations are obliged to store the information that they hold in a good, structured and accessible way. This implies that also archivists are being faced with this new medium. Next to the Archive Act, also the Access Laws and the Privacy Laws arrange how government administrations are to deal with the information they receive and compose. It will be shown further on in this report that also digital data including electronic mail falls under the application of these rules and that it has to be treated accordingly.

The fact that employers have made e-mail available to their employees has given birth to a number of legal questions. There is a great legal uncertainty about the issue as to what extent the employee's right to privacy can be put aside for the employer to be able to exercise his right to check the work being performed[2]. Also an archivist needs to respect the Privacy Laws and wonder to what extent the electronic mailbox of a civil servant is a house of glass. It will be shown further on that it is not the principle of confidentiality of mail but the principle of secrecy of telecommunication that considerably limits the rights of the archivist. We will also investigate how the Access Laws influence the e-mail policy of government administrations.

Most legal questions about privacy and access do not have ready-made answers. It is therefore important that governments compile clear guidelines so that directors, civil servants and network managers know what they have to live up to and can adapt their behaviour. Because of the growing use of e-mail on the work floor and the lack of relevant jurisdiction most organisations have started working on 'e-mail policies'. We notice however that most of these policies do not contain guidelines concerning the organisation's policy about archiving e-mails[3]. They deal mostly with the access rights to the e-mail

---

1 http://www.fedict.be

2 This legal question is discussed extensively for Belgian legislation in DUMORTIER, J., 'Internet op het werk: controlerechten van de werkgever', *Oriëntatie*, February 2000, 35-42 and DUMORTIER, J., 'Little Brother is watching you: mag de werkgever het Internetgebruik van zijn werknemers controleren?' in X., *Liber Amicorum Prof. Dr. Roger Blanpain*, 1999, 243-259.

3 An example of a 'telecommunication policy' that does consider the record-keeping aspect of e-mail is the model presented by WHITMAN, TOWNSEND and AALBERTS. WHITMAN, M., TOWNSEND, A. and

system for certain categories of employees, the correct use of e-mail by the employee (how a message should be composed, e-mail etiquette, forbidden usage), the privacy expectations employees can have or not (especially this part needs to be evaluated from a legal perspective), virus protection, copyright guidelines, etc. The first part of this report discusses the current legal framework about (archiving) e-mail so that this can be taken into account when developing an e-mail policy.

The widespread usage of e-mail causes more than only problems of a legal nature for the archivist. He or she is expected to incorporate these electronic records into his archive and to keep his e-mail archive in a good, structured and accessible state. The second part of this report will therefore deal with the problem of archiving e-mail. We will take a close look at what possibilities exist to archive e-mail and we will give guidelines for their practical application. The evolution towards e-government and e-commerce underlines the importance and the possible archive value of e-mail even more. And yet only few institutions or organisations possess a coherent archive system for incoming and outgoing e-mail messages. An archiving policy therefore needs to be developed urgently.

Continuing from the conclusions of the legal preparatory study first all archiving possibilities will be looked into. Attention will be paid to the choice between printing or digital archiving, the metadata and the transmission data of e-mails, attachments, electronic durability, integration with related documents, access and secure storage. This part will offer a few archival and technological building blocks for the e-mail recordkeeping system. Both will greatly influence the archiving process. Other determining factors are the e-mail policy, the organisation and the IT-infrastructure of the creator. An efficient archive system needs to be tuned according to these factors. As the e-mail policy and the organisation differ for each institution a wide range of alternative good recordkeeping systems will be available. An example in the form of a good practice will be presented.

Sofie Van den Eynde wrote the juridical part of this DAVID-report. Filip Boudrez was responsible for the part on archiving.

Leuven - Antwerp, July 2002

AALBERTS, S., Considerations for an Effective Telecommunications-Use Policy, Communications of the ACM, Vol. 42, June 1999. CARDEN compares the *ABC telecommunications' Electronic Mail Policy* that became available mid 1999 on the Intranet site of ABC to the model and concludes that also here nothing is regulated concerning the storage of e-mail. Available on http://science.kennesaw.edu/csis/msis/stuwork/IS8070_pa.htm#policy

An example of an *e-mail policy* from the public sector that does not refer in any way to the treatment of e-mail as official documents is the *Internet and E-mail policy* of Washtenaw County, Michigan. See http://www.co.washtenaw.mi.us/DEPTS/LIB/LIBINPOL.HTM

I. WHAT IS AN E-MAIL?

We will start this report with a brief introduction of the phenomenon 'electronic mail'. Readers who are well acquainted with e-mail as for example daily user can skip this section and go directly to Part III.

Electronic mail or 'e-mail' in short allows the quick and easy exchange of messages with other Internet users, on the condition that both sender and receiver possess an e-mail address and an Internet connection. The term e-mail refers both to the system that transports these messages electronically and to the messages themselves. In this report the term 'e-mail system' will refer to mail server (software), while the term 'e-mail' will be used as a synonym for an electronic message.

A. HOW DOES E-MAIL WORK?

Every person on the Internet possesses his or her own e-mail address that is always structured identically. It consists of two parts that are separated by the '@' sign, pronounced as the English "at". The part before the at-sign is called the user name or the e-mail name; the part after the at-sign is called the domain. The domain is determined by the domain name of the Internet provider[4]. When a receiver Peter Petersen has opened an electronic mailbox with Hotmail, his e-mail address could look like "peterpetersen@hotmail.com". Many Internet providers are active on the Internet which makes the competition considerably big.

Special software is used by the Internet provider to conduct all this electronic messages traffic in a structured way. This special software is called "mail server software" (for example Exchange Server, Domino Server). Two types of mail server exist: one for sending messages (the SMTP server) and one for receiving messages (the POP server). The SMTP server ('Simple Mail Transport Protocol') directs all sent messages to the correct destination[5]. This can be best compared to post office sorters. The Internet does not have pick-up times: messages are delivered without delay. The POP server ('Post Office Protocol') receives the messages and puts them in the appropriate electronic mailbox. This server plays the role of mailman putting the letters in the correct mailbox too. The electronic mailbox is a reserved folder on the mail server of the Internet provider. It stores the e-mails until the receiver collects them. Access to this electronic mailbox is secured by a password. This avoids everybody being able to empty one's mailbox and read one's messages.

---

[4] The domain name of the Internet Provider can often be found in its Internet address, for example www.hotmail.com, www.uunet.com.

[5] SMTP is one of the protocols used to send e-mail. Next to that there is also for example X.400 and X.500. Networks have other configurations than e-mail that takes place via a dial-up connection (IMAP).

The 'mail client' or the e-mail programme is the software used to write messages, send electronic mail, empty mailboxes and read or print messages. Many different e-mail programmes exist, for example Eudora, Outlook, Happymail etc.

B. STRUCTURE OF AN E-MAIL MESSAGE

All e-mail messages share the same structure, whatever e-mail programme is being used.

From: contains the e-mail address of the sender: sender@provider.be

To: contains the e-mail address of the receiver: receiver@provider.be

Subject: contains the subject of the electronic message

Cc: 'Carbon Copy'. The sender can use this field to fill in the e-mail address of other persons who will receive the message as well. All receivers can read each other's e-mail address.

Bcc: 'Blind Carbon Copy'. The same goes here as for Cc, but the difference is that the receivers do not see each other's e-mail address so that they do not know from each other that they have received the same e-mail.

Attached: Complex electronic documents such as documents composed using a text processor, calculations programmes or graphical software are usually connected to the e-mail as 'attachments'. Even sound and image files can be sent this way. The actual message is often no more than a few accompanying words or sentences. An attachment is an integral part of the electronic message.

All this information is contained in the 'header' of the message. Most e-mail programmes have the possibility to indicate in the header that the e-mail needs to be protected for example via encryption or that the e-mail needs to be treated by the receiver with priority. The 'body' of the e-mail only contains the actual content of the message.

C. ADVANTAGES OF E-MAIL

E-mail does not only replace part of the informal, oral communication but it also takes over part of the formal correspondence that takes place via the internal correspondence of an organisation or via the regulated postal service of 'De Post'. Compared to a normal letter, sending an e-mail has a number of advantages:

1. Sending an e-mail goes much quicker. The e-mail has reached the addressee's electronic mailbox within a few seconds to a few minutes after it has been sent.

2. Sending an e-mail is much cheaper. This is especially the case when an e-mail replaces a letter one wants to send to an addressee in another country. The price of an e-mail is constant, whether it is being sent to one's neighbour or to someone on the other side of the world.
3. Sending an e-mail can be done at every moment (e-mail is also being sent on Saturday and Sunday) and one does not even have to leave the house to do so.
4. Sending an e-mail to multiple persons takes up almost the same time as sending it to one person.
5. E-mail can be read any time and anywhere, as long as an Internet connection is available. The electronic mailbox is accessible anytime and anywhere.

II. WHY ARCHIVE E-MAIL?

Before looking into the legal framework we need to wonder why archiving e-mail has currently become such a big issue. Put differently: why archiving this relatively new type of digital information when it is not even clear how electronic documents must be archived even though they have entered modern society a long time ago. Furthermore, the introduction of applications such as e-mail has led many organisations to increase the amount of information they store. E-mail has indeed not just replaced some classical means of communication such as letter correspondence and telephone conversations, it is especially an extra means of communication that is complementary to existing means of communication[6]. This implies that many organisations need to archive more information than before. However, it would be a mistake for records managers and archivists to deny the existence of e-mail.

A. E-MAIL AS A RECORD

Is an electronic message a record or not? The answer to this question is important. It determines whether or not e-mails fall within the scope of the science of archiving. Should archivists and records managers be consulted for the composition of an organisation's e-mail policy? When compared to a telephone conversation, it becomes obvious that e-mail must be considered as a record.

The global flow of information increases the importance of international standards for archiving terminology. This was one of the findings of the 14th Congress on Archives, held in September 2000 in Seville, Spain. That is why the DAVID project adopts, as much as possible, generally accepted definitions of archiving terms. A universally accepted definition of the concept 'record' in an archiving sense could be: *"A document, recorded in whatever format or medium, created or received by an agency,*

6 WALLACE, D., Recordkeeping and Electronic Mail Policy: The State of Thought and the State of the Practice, paper prepared for the Annual Meeting of the Society of American Archivists, Orlando, Florida, September 3, 1998, available on http://www.rbarry.com/dwallace.html. The separate legal statute of e-mail will also appear in the analysis of the applicable legislation.

organisation or person in pursuance of legal obligations or in the transaction of business."[7] An analysis of the actions and procedures of e-mail demonstrates that it complies perfectly with this definition.

- E-mail is recorded, be it on the Internet provider's server or be it on the hard disk of the receiver's computer. Here lies the difference with a telephone conversation and a website visit. Both are also types of telecommunication, but the content of the telecommunication message is not stored on a carrier. These types of telecommunication are casual.
- Created: there is no difference here with traditional records. An e-mail that has been composed but never sent (UNSENT) is a record from the person who has composed the e-mail.

  In the paper world those pieces that are created within the organisation are called 'internal pieces'. An 'internal e-mail' is therefore an e-mail sent to a person within the proper organisation[8].

  Received: there *is* a difference here with traditional records. In the paper world an item that an organisation receives is a record of the receiving organisation and no longer of the sender. An archive record will only remain with the sender if a copy has been made and stored. A sent e-mail however normally remains present with the organisation that has composed it in the so-called 'outbox'. It is an item that has been composed (and sent) by that organisation and will become part of its archive. The e-mail will also be part of the receiving organisation's archive.
- In pursuance of legal obligations or in the transaction of business: here the problem of personal usage of the organisation's e-mail system is situated. Many employees use the e-mail system also, to some extent, for personal reasons. Only those e-mails that result from the functioning of the organisation can be considered to be records. Also e-mails that are not specifically addressed to the organisation and that reach its mailbox by accident or unsolicitedly do not form part of the archive[9]. An example of this is 'spam' [10] or messages originating in electronic mailing lists that contain the e-mail address of the organisation by accident. These e-mails form part of the archive of those who have sent them.

---

7 ISO 15498. See also 5127 Information and Documentation Terminology. ISO International Standard 15489 was prepared by Technical Committee ISO/TC 46, Information and Documentation, Subcommittee 11, Archives/Records Management, in response to consensus among participating ISO member countries to standardise international best practice in records management, using the Australian Standard 4390 as a starting point.

8 An e-mail sent to a person within the organisation is obviously also a record.

9 Commercial printing and elections propaganda are examples of paper documents that are not records as they have not been received because of the activities of the organisation or to maintain its rights.

10 'Spam' can be defined in many ways. A general definition would be 'information that has been sent to multiple receivers who are unacquainted with the sender and who have not asked for this information'. Most 'spamming' takes place by e-mail. Some legal guidelines have been composed on the European level that Member States should enforce to limit the appearance of spamming. According to Article 7.1 of Directive 2000/31/EC of 8 June 2000 concerning certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on Electronic Commerce') Member States must take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail regularly consult and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves to. With respect to unsolicited e-mail undertaken by other persons, Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunication sector leaves it open to the Member States to choose between opt-out or opt-in. As a result of this a system of divergent regimes came into existence that is unworkable in the internal market. Direct marketers in opt-in countries may not target e-mail addresses within their own country but they can still continue to send unsolicited commercial e-mail to countries with an opt-out system. Furthermore, e-mail addresses very often do not indicate the country of residence of the recipients. That is why the revised draft

In 1998 the results were published of a study conducted at the *Graduate School of Library and Information Science* at the University of Austin, Texas. The goal of this study was to investigate the state of the art of the considerations regarding, and the development of, e-mail policies, both in the public and the private sector[11]. Building on the results of this study DAVID WALLACE has investigated a number of e-mail policies with regard to their 'archive value'. For a collection of 38 e-mail policies from all over the world he looked at the extent to which the archiving of e-mail was part of the policy. It is important to realise that WALLACE only selected those e-mail policies that already prior to his investigations had demonstrated that they considered archiving questions as an important issue of the policy[12]. The situation regarding "ordinary", randomly selected e-mail policies is therefore not as optimistic as the one regarding the investigated policies, even as also for these last ones the results are not as good as expected, as shall be demonstrated further on.

Only 60% of the researched policies mention the status of e-mail as a record. Even though most policies are not very explicit and only mention that an e-mail *can* be a record of the organisation, there seems to be a general consensus about the fact that e-mail is not just an informal means of communication but can result in records. It *is* generally mentioned in those policies that discuss the status of e-mail that the used technology or the e-mail format is irrelevant and that the criteria to determine whether an e-mail is a record need to be identical to those that apply to paper documents. Only 60% of the policies that discuss the status of e-mail give some criteria to distinguish records from non-records. The purpose (for example e-mails in which a decision is taken, e-mails that give permission to something) and the type of e-mail (for example correspondence, minutes of a meeting) are the most common criteria. The other policies put the decision to qualify the e-mail with the end user. The opinion that neither those e-mails whose content is not related to the activities of the organisation nor those that are personal e-mails are records is generally present in these policies.

That e-mail can form records is also shown from the e-mail etiquette rules that are published all over the Internet. They indicate how a civilised e-citizen should conduct oneself regarding the electronic message traffic. Most of these codes of conduct contain guidelines about the composition and the form of an e-mail message and about sending attachments. Some point at the importance of living up to these rules as e-mails may be archived at a later stage[13].

Now that we have learned that e-mails can be considered as records of an organisation as long as they are established in the framework of the organisation's activities (= **functional e-mail**), we have to wonder if these new-type records have any permanent archive value. As a principle the same rules apply to e-mail

---

version of Directive 97/66/EC obliges the Member States to adopt an opt-in system. This measure will reduce spamming to a significant extent. In the U.S. the Electronic Mailbox Protection Act of 1997 deals with the issue of unsolicited e-mail.

11 The results of this study '*Managing E-mail as Records*' have been published on the following URL: http://www.gslis.utexas.edu/~scisco/lis389c.5/email/index.html

12 An overview of all researched policies is available on http://www.rbarry.com/dwallace.html

13 http://www.larrysworld.com/articles/emailete.html

that apply to other records. This implies that only a small percentage of all e-mails will have to be stored. We will give two examples here, one from both the public and the private sector[14].

B. ARCHIVE LEGISLATION

The government does not have a free choice about storing or destroying its records. Most countries have Archive Acts stipulating that administrations shall not remove, deface, alter or destruct records in the custody of that administration.

As far as an e-mail is a record of these governments, it is subject to the Archive Act. Archive legislation does not consider e-mail as a purely informal means of communication, only intended for personal usage.

The most visible discussion about the statute of e-mail arose in the United States in 1989 around the known 'PROFS' and 'GRS 20' trials. The e-mail policy of the federal administration enforced all civil servants to print all those e-mails that could be qualified as a document in the sense of the *Federal Records Act.* Later the decision was taken to destroy the electronic version of all e-mails. Stating that the electronic versions of e-mails are only extra copies and no official government documents motivated this decision. The federal administration felt it had fulfilled its duties under the *Federal Records Act* by only storing the paper versions of e-mails and deleting the electronic versions without prior consent from NARA[15]. The *Federal Records Act* only imposes the obligation to store government documents.

A number of pressure groups[16] summoned the federal administration and were proved right. After ten years of legal dispute the original judgement of Judge Charles Richey was confirmed[17]. The contradictory administration reasoning (that an e-mail legally speaking can be a record but that it still can be destroyed) was waved aside. According to the judge the electronic version of an e-mail is the only legal record as the printed version does not always display all information that is contained in the electronic version (context information like the date and time of sending and the identity of the receiver are often not mentioned on the screen but do form part of the e-mail message). The form of a record is irrelevant, the judge added. This judgement does not only mention the possible formal character of electronic messages within the government, it also indicates how they should be stored: in their original, electronic form.

The Court of Appeal of the district of Colombia however reviewed this judgement on 6 August 1999. The Supreme Court refused a final request of the pressure groups to reverse the decision of the Court of

---

[14] For an elaborate overview of the reasons why records are being preserved see VAN DEN EYNDE, S., *Electronic archiving: legal issues in a Belgian perspective, part 1*, Leuven, Interdisciplinary Centre for Law and Information Technology, 88 p. (available in Dutch only).

[15] NARA (National Archives and Records Administration) is a federal department that has legal authority to supervise all federal documents in the United States (http://www.nara.gov).

[16] Among others The Organization for American Historians, as well as individuals such as writers, researchers and journalists.

[17] Armstrong et al. vs. Executive Office of the President et al. (Civil Action No. 89-0142); Public Citizen, Inc. et al. vs. Carlin et al. (Civil Action No.96-2840)

Appeal. Therefore no fundamental decision has been made, so that it remains uncertain whether e-mails can be stored as paper prints[18].

The legal value of these cases for Belgian archives is merely illustrative. Yet they give a clear view on the content of the current discussion about storing e-mail, a discussion that is not yet prominent in Belgium and that we want to kick off using the DAVID project. In agreement with the original judgement by Judge Charles Richey we believe that e-mails can best be archived digitally and not as hard copy[19]. However we do not have indisputable legal arguments for this.

Article 7 of the Dutch Archive Act of 1995 clearly determines that the caretaker has authorisation to replace records by reproductions and to destroy the records that have thus been replaced. This fundamental regulation stems from the lack of storage capacity within the State Archive[20]. Microfilming is without any doubt the most well-known of these substitution measures. But should this regulation be used to avoid the problems concerning digital archiving? Is it allowed to destroy original digital records to the benefit of paper substitutes? Article 5 of the Belgian Archive Act stipulates (as most Archive Acts) that permission of the General State Archivist is needed if the government wishes to delete records. It is therefore this General State Archivist who is authorised to make the final decision about whether e-mails should be stored in their original electronic form or that a paper print suffices for long-term storage. He is also authorised to determine the conditions under which the original electronic version may be destroyed. Currently no regulation has been introduced in Belgium about this.

Nothing prevents the electronic mailboxes of civil servants from being printed and stored on paper *as well*, but we consider this only as a possible additional storage measure. Three arguments can be used to support this. The first is a *fundamental argument*. E-mails are by definition electronic. Most Archive Acts intend the original electronic version to be archived. In the past the Belgian General State Archivist has ruled about the scanning of letters. A paper letter with archive value, he stated, can not only be stored in digital form. The paper original needs to be stored as well. Secondly there are *practical reasons* to exclude storage only on paper. Some elements from the electronic context cannot be transposed into a paper environment. There is for example the digital signature, based on the bit serial of the e-mail content, which would be lost when transposing to printed text. And finally also the *logical argument* goes that a digital world requires digital archiving methods because of its many benefits.

The formal character e-mail may have is also demonstrated in the current European discussion concerning e-government, both on the European Union level and on the Member States administration level. E-government is an important political issue. The e-portal should allow every citizen to contact the government formally by electronic means. It goes without saying that electronic mail is very much suited for this. The Belgian Presidency and the Commission jointly organised a high-level ministerial conference on e-government applications on 29-30 November 2001 in Brussels. The conference demonstrated the current European position in this fast-moving area and also provided a framework to

[18] More information about this is available on http://www.nara.gov/records/grs20.

[19] A 'hard copy' is a print on paper.

[20] Archive Act, Explanatory Memorandum, Chamber Pieces II, 1992-1993, 22 866

address e-government issues beyond the 2002 eEurope Action Plan.[21] The establishment of an e-Commission is one of the objectives set in the context of the e-Europe Action Plan. All basic transactions with the European Commission must be available on-line (for example funding, research contracts, recruitment and procurement). The Member States on the other hand have committed themselves to ensure generalised electronic access to the main basic public services by the end of 2002. The Internal Market Council adopted a list of 20 basic services for citizens and businesses elaborated by the e-Government work group in March 2001[22]. In this era of electronic government it is hard to claim that the Archive Acts would not apply to information the government receives via digital channels. The government has reason to investigate adequate security measures: both the citizen and the government wish to have certainty about the authenticity and integrity of electronic messages.

C. GOOD OPERATIONAL MANAGEMENT

E-mail has become a formal and informal communication channel for all levels of companies, government departments and institutions. Communication that previously took place by telephone or by letter is now taking place by e-mail. Some procedures and transactions within these organisations will therefore reflect in electronic messaging. To allow later reconstruction of these procedures and transactions it is important that these electronic messages are stored in a structured and accessible way. The content of an e-mail can reflect the status of a given case, it can contain the minutes of a meeting where important decisions have been made or where tasks have been divided, or it can simply contain information that may be relevant later to oneself or a colleague (such as a web link). Not selecting these e-mails for storage or deletion in an efficient way may have a negative effect to the efficiency of the operational management.

An important reason for many organisations not to archive e-mail is the legal risk that is associated with storing e-mails for too long a period. The idea is that e-mails can be used as evidence in the conduct of a case against an organisation and thus may form more a threat than a contribution to the stability within an organisation. An American company experienced this when an employee conducted a trial to dispute his dismissal. The official reason was that he did not meet the demands. *Electronic Evidence Discovery Inc.*[23] however gained access to more than 750 000 e-mails in the back-ups of the e-mail system of the company that still contained previously deleted e-mails. They demonstrated that the employee indeed was not dismissed for not meeting the demands.

We however feel that the advantages of permanent e-mails storage are greater than any possible disadvantages.

Now that we realise the possible importance to store an organisation's e-mails, the question arises whether some control can and should be exercised to an end user's deletion of e-mails. Specific to this

[21] http://europa.eu.int/information_society/eeurope/action_plan/egov/index_en.htm

[22] The official Belgian e-government can be accessed via http://www.government-online.be/default.htm with interesting links to e-government projects within other Member States.

[23] *Electronic Evidence Discovery* offers services in the field of recovering electronic evidence during a trial and in the field of reducing the risk of discovering such evidence before a trial (http://www.eedinc.com/index.html).

type of communication is that the user can store or delete any incoming or outgoing e-mail according to his own insights, without the need to consult other persons. E-mail does not follow the traditional rigid streams of information within the organisation, so that information islands appear[24]. Are these islands private property of the employee or can archivists and records managers perform some surveillance to prevent the unjustifiable deletion of e-mails? We also need to discuss the question whether an employee is allowed to send and receive strictly personal e-mails.

We will now investigate what legislation applies to (the archiving of) e-mail. The following analysis will demonstrate that some legal rules conflict with the practical application of archiving e-mail. It is common that some control is exercised by the responsibles for the correspondence and the organisation archivists. This analysis should allow determining the conditions under which it is justified to exercise control on the storage and deletion of e-mail by the end user.

III. THE LEGAL VALUE OF E-MAIL

The legal value of e-mail needs to be determined for a policy to be developed in the field of sending formal e-mail. Formal e-mail messages are records in the sense of national Archive Acts (thus functional e-mail) that will usually be stored because their content has (legal) consequences for the government, because they have evidence or liability value or because they matter for the correct interpretation of other data. All other e-mail is then informal e-mail. The e-mail policy of the government needs to determine whether the electronic sending of formal e-mail is permitted or that a written document needs to be sent.

E-mail is a new means of communication. To determine the legal statute of an e-mail we need an existing means of communication that is similar to it. We can best compare e-mail to a letter. A letter is defined in the dictionary as "a writing in the shape of an announcement, a message, aimed at one or more non-present persons, to let him (them) know something, closed and bearing an address when sent". The current legislation allows also electronic data to form a writing as far as they are stored in a more or less sustainable way. Furthermore the e-mail sender also wants to transfer a message to persons non-physically present. An e-mail message always bears an (e-mail) address and when the e-mail has been encrypted it is also closed, being non-accessible to others during the transfer.

It is the content of a letter that determines its value, and this applies to e-mail too. There are two possibilities, based on the existence of possible legal consequences or not. The law can dictate some formal requirements for the first category of e-mails.

[24] TOMER, C. and COX, R., 'Electronic Mail: Implications and Challenges for Records Managers and Archivists', *The Records and Retrieval Report 8*, November 1992, No° 9, 3-4

A. THE E-MAIL IS LEGALLY BINDING

The content of the e-mail (or of the succession of e-mails) can aim at having legal consequences. That implies that it can change the legal situation of the parties (citizen-government, government-government). The formal e-mail has been composed with a future purpose as evidence. Many types of documents are subordinate to certain formalities for evidential reasons. Therefore, evidential law is decisive for the way we archive documents. The most common formality is the requirement of a signature. Many European countries require a proof that non-commercial transactions are embodied in a signed document[25]. Until recently it was unclear whether a judge would accept electronically signed documents.

Since the European Directive 1999/93/EC of 13 December 1999 concerning a Community framework for electronic signatures came into force[26], Member States must give so-called "qualified electronic signatures" the same legal effect as hand-written signatures. These are electronic signatures that meet a certain security standard, which is further specified in the annexes to the Directive. As a result, transactions that require a signed document for proof can now be effected by electronic means, such as electronic mail.

Other formal requirements the law may prescribe are the necessity of a writing or the presence of some obligatory stipulations in the document. The recent e-commerce Directive 2000/31/EC of 8 June 2000[27] states in its Article 9 that the Member States must ensure that the legal requirements that apply to the contractual process (the archival phase included) neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity because of their electronic origin. E-mails calling contracts into being may thus not be rejected as proof by the Member States simply because of their electronic nature.

B. THE E-MAIL IS LEGALLY NOT BINDING

This applies to most e-mails sent by the government, usually formal mails that do not have formal requirements to live up to due to the lack of a legal transaction. Most formal e-mails contain legal facts (sensu stricto[28]). These are facts with some legal implication. They can consist of an answer to a request for information through which the government engages to its liability. Factual elements can be proven with all possible legal means according to the legislation of the Member States[29]. In this case the e-mail will be qualified as a normal writing.

---

25 KÖTZ, H., *European Contract Law: Formation, Validity and Content of Contracts, Contract and third parties*, Oxford, Clarendon, 1998, 78

26 Official Journal of the European Communities, L13/12, 19 January 2000

27 Official Journal of the European Communities, L178/1, 17 July 2000

28 Legal transactions form part of the legal facts in their broadest sense. After excluding legal transactions from this category only legal facts in the strict sense remain.

29 De Lamberterie, I., *La valeur probatoire des documents informatiques*, Rapport de synthèse, September 1990

The reason for sending a message on paper rather than electronically is usually that some legal conditions exist about the format that can only be met on paper. On the European level, many legislation initiatives are currently taken to delete these formal requirements from legislation[30]. All other messages can be sent electronically. We hold the opinion that this is appropriate when the citizen has contacted the government individually and in a regulatory manner via e-mail. The citizen can reasonably expect an electronic answer if the government takes its electronic image seriously.

IV. PRIVACY: LEGAL FRAMEWORK

A. THE FREEDOM TO ENGAGE IN TELECOMMUNICATION

The employers' double usage of the e-mail system (professional and private) does not make it easier for the company to distinguish records from non-records. From an archivist point of view it would be much better if all e-mails within an organisation were professional. This could be realised for example by asking employees to conduct their personal e-mail correspondence via a personal e-mail address and not via the e-mail address an employee possesses for an efficient exercise of his or her professional activities.

Engaging in a work relation does not cause the employee to lose his freedom to communicate. The freedom to communicate is a constitutional right that is protected by Article 8 of the European Convention for the Protection of Human Rights (E.C.H.R.) and implies that one, also in a work relation, needs to be allowed the freedom to start or receive communication or not.

This principle was first worded in the jurisdiction of the European Human Rights Court in the *Niemitz judgement* [31]: *"Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. It is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world*." This principle was later confirmed in the Burghartz judgement of 22 February 1994[32].

---

30 For example Directive 99/93/EC of 13 December 1999 concerning a Community framework for electronic signatures (Official Journal of the European Communities, L13/12, 19 January 2000); Article 9 of the E-commerce Directive 2000/31/EC of 8 June 2000 (Official Journal of the European Communities, L178/1, 17 July 2000): the Member States must ensure that the legal requirements applicable to the contractual process (the archiving phase included!) neither create obstacles for the use of electronic contracts, nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.

31 *Niemitz vs. Germany*, ECHR, 23 November 1992, Series A, No. 251/B, para. 29

32 *Burghartz*, ECHR, 22 February 1994, Series A, No. 280/B, para. 24 : "*private life conceived of as including, to a certain degree, the right to establish and develop relationships with other human beings, in professional or business contexts as in others*."

Does the freedom to engage in telecommunication imply the liberty to use the means of communication the employer puts at an employee's disposal for personal communication? There is not a general principle that does not allow the employer to forbid private use of the means of communication that he has made available. After all, he or she owns them[33]. On the other hand it can be stipulated that employers need to demonstrate some tolerance regarding private communication that takes place via their means of communication, especially because the work floor is the best place to maintain contacts with colleagues and even with outsiders. The extra problems this causes for selecting and storing e-mails are not enough cause to limit this constitutional right.

The constitutional freedom to communicate is obviously not unlimited (no constitutional right is). The employee needs to be available to the employer during the work hours to exercise his or her work tasks. The employee's private communication may not hamper the execution of the labour contract.

B. E-MAIL PRIVACY: A FUNDAMENTAL RIGHT?

Even when it is clear that an employee only sends and receives professional e-mail, the question remains whether the records manager is allowed to transfer these e-mails autonomously and without the employee's knowledge into the electronic archive management system or may print them for storage in the paper archives.

E-mail etiquette often contains the recommendation that it is better not to write in an e-mail what you do not want others to know or what you normally would not say in public, but to discuss such matters from person to person or by telephone. It is said that the employer would view e-mails for all sorts of purposes, including archiving. These conduct codes try to convince the reader that '*there is no such thing as a private e-mail*'. But is this so? Is your electronic mailbox a house of glass that is accessible to everyone with the technical possibilities, or should the content of an e-mail remain a secret, even for archive purposes?

1. Most relevant international instruments

To answer these questions employers, archivists and records managers can use several instruments. First of all, there is national data protection legislation that has to be complied with. In this report we will focus on the most relevant international instruments to judge the issue of e-mail privacy:

- Article 8 European Convention for the Protection of Human Rights and Fundamental Freedoms (E.C.H.R.)
- Directive 95/46/EC concerning the protection of individuals with regards to the processing of personal data and the free movement of such data

[33] Some doctrines heavily criticise this theory: a.o. DE HERT, P., 'Violation of the confidentiality of (tele)communication in professional relationships', *Tijdschrift voor Sociaal Recht*, 1995, 213 (in Dutch).

- Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunication sector

2. Article 8 E.C.H.R.: Telecommunication secrecy as a fundamental right

a) History of the secrecy of telecommunication as a fundamental right

The right to secrecy of telecommunication is generally recognised in Article 8 of the E.C.H.R. [34]:

> ARTICLE 8 E.C.H.R.:
>
> 1. Everyone has the right to be respected for his private and family life, his home and his *correspondence.*
> 2. There shall be no interference by any public authority regarding the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The European Convention on Human Rights is an instrument that was prepared and negotiated within the institutional framework of the Council of Europe. This Council of Europe, established in 1949 in London by ten western European states, has as its goal to harmonise the policy of its Member States and to introduce common norms and practices. To achieve this the Council brings together parliamentarians, ministers, government experts, local and regional representatives, youth organisations and INGOs (International Non-Governmental Organisations) on a number of levels to exchange knowledge and experiences. The Member States already possess a foundation of more than 170 European treaties to adapt and harmonise their legislation. The treaties cover a wide variety of topics: from protection of computer data, hooligan violence and nature protection to social security, cultural co-operation and prevention of torture.

The European Convention on Human Rights aims at giving the principles determined in the Universal Declaration of Human Rights a collective and enforceable status. The Council of Europe has developed a unique legislative system that allows Member States or individual citizens to file a complaint at the European Human Rights Court against Member States that do not respect the treaty. This has resulted in a large collection of jurisdiction from the European Human Rights Court.

The principle of secrecy of telecommunication dates back a long time in Europe. The principle of confidentiality of mail was recognised for the first time in 1831 in the "Constitution of Hesse" of the

[34] The full text of the convention is available on http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

German principality of Hesse. Even though the text explicitly refers to "das Briefgeheimnis" [the letter confidentiality] it protected not only letters but also the content of all correspondence that took place by mail. The mail confidentiality principle in this stage only applied to the relation between citizen and government. In the second half of the nineteenth century the legislator was confronted with new means of communication such as the telegraph and the telephone. New constitutions that later arose all over Europe also recognised these new means of communication.

In the U.S. on the other hand the existence of a telecommunication secrecy principle is the result of the interpretation of the Fourth Amendment as a regulation protecting privacy. The Fourth Amendment states that the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall be issued but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized. The Fourth Amendment was a reaction to the phenomenon of general search warrants in the America of the eighteenth century. General warrants were often used to find evidence in the archives of suspects of political crimes.

The American courts have attributed an interpretation to the Fourth Amendment beyond these specific circumstances. By applying it to *all unreasonable* searches and seizures a general constitutional right to privacy was deducted from this stipulation[35]. Also those cases where telecommunication was intercepted were always brought to trial as cases of unreasonable searches and seizures[36]. The constitutional protection of the telecommunication secrecy has therefore been established as part of the right to privacy and not as an autonomous right.

b) Scope of the constitutional principle of secrecy of telecommunication

Article 8 provides protection against arbitrary (that is: unjustified) interference with an individual's correspondence. However the treaty does not further explain the concept "correspondence". The doctrine has usually given a literal interpretation to the concept. Only written correspondence fell in this interpretation under 8 E.C.H.R.[37] The Court however ruled the term "correspondence" as encompassing all forms of telecommunication[38]. In the case of Klass vs. Germany [39] the Court determined that Article 8 is protecting telephone conversations as well as written correspondence. Whether this protection extends to e-mail messages remains unsure but the principles (of protecting written and *tele*communication) would support such a protection[40].

---

35 RUIZ, B., *Privacy in Telecommunications. A European and an American approach*, The Hague, Kluwer Law International, 1997, 86

36 Maryland Penitentiary vs. Hayden, 387 US 294 (1967)

37 FAWCETT, J., *The Application of the European Convention on Human Rights (Article 8)*, Oxford, Clarendon Press, 1987, 228

38 RUIZ, B., *o.c.*, 142

39 *Klass vs. Germany*, ECHR, 6 September 1978, Series A, No. 24, para. 41

40 On-line Rights for On-line Workers in Member States of the European Union, Report on a Research Project for UNI Europa, European Commission, 15 November 2000,

The secrecy of telecommunication is also protected when this telecommunication takes place in the work place. In the Niemitz case the European Human Rights Court argued that *"there appears to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not."* Sir Niemitz was a German lawyer who filed a complaint against the German State who had searched his office in order to find letters that could incriminate another person without respecting the secrecy of telecommunication principle that was guaranteed under Article 8 E.C.H.R.

In the case of Halford vs. UK the former Assistant Chief Constable of Merseyside police complained that her private calls from work were being intercepted. The UK government tried to argue that as the calls were made from the workplace, Article 8 did not apply. The European Human Rights Court rejected this. It held that an employee has a reasonable expectation of privacy in the absence of any advance notification that interception might take place[41].

Several national courts have also supported this point of view regarding the applicability of the secrecy of telecommunication principle in the workplace. Recently the French Supreme Court decided that employers could not read employees' electronic correspondence[42]. This applied even if the employer has prohibited private use of his computer system. The Court referred to Article 8 of the E.C.H.R. This regulation however does not prohibit companies from accessing employee electronic messages in all circumstances, provided that there is no invasion of privacy. If an employer needs access to the mailbox of employees, he must clearly outline when and how he will do so for example for archival purposes. Employers therefore better compose an e-mail policy that predetermines the rules for the usage of the e-mail systems. It must be made perfectly clear to what extent employees can have a reasonable expectation of privacy.

As we have pointed out, the European Human Rights Court has taken a strong stance in favour of the protection of the right to secrecy of telecommunication. A current American law case dealing with an employee's right to privacy versus a company's legitimate business interest in investigating employee e-mail shows however that US courts generally tend to protect the company's interest. Most courts have decided that the interests of the company outweigh an employee's expectation of a right to privacy. From the Fourth Amendment search and seizure interpretation as a right to secrecy of telecommunication, the "reasonable expectation of privacy" has been extended to purely private employer/employee relationships. In McLaren vs. Microsoft Corporation (28 May 1999) an employee who transmitted e-mail

http://www.unionnetwork.org/uniibits.nsf/172541a5444b8445c1256811002a0302/061b38ba2eca776dc1256a2b0048e644?OpenDocument

41 Halford vs. UK, ECHR, 25 June 1997, No. 73, para. 45

42 Cour de Cassation (Fr.), Nikon France vs. Onos, 2 October 2001, Arrêt No. 41-64

messages over the company network and stored the message in (even!) personal folders did not have a reasonable expectation of privacy regarding those messages.

The fact that the U.S. never had an explicit constitutional protection of telecommunication and the fact that this is only a deduced right are probably no strangers to this.

3. Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunication sector[43]

The principle of secrecy of telecommunication is also protected on the European level by Directive 97/66/EC. This Directive turned the principles of Directive 95/46/EC (the Privacy Directive: see further) into specific rules for the telecommunication sector. The Directive originated in the greater troubles that occurred regarding the automated storage and processing of personal data in the telecommunication sector, and also to harmonise the different rules in the Member States in order not to hamper the functioning of the internal market. The Directive obliged the Member States to use national legislation to guarantee the confidential nature of communication and related personal data. They should forbid any monitoring, wiretapping, storing or any other interception or control of the communication and related personal data by persons other than the users, if these persons have not given prior consent (Article 5 of the Directive). The aim of this stipulation was to protect the secrecy of telecommunication specifically for the telecommunication sector according to the E.C.H.R. and according to the different constitutions of the Member States. For an organisation's storage of e-mail this implies that the archivist or the records manager needs prior authorisation of the e-mail communication partners. It is difficult however to determine how to get the communication partners' permission. Sometimes it is difficult to find out who are those communication partners, for example if the addressees are all mentioned in Blind Carbon Copy. The solution could be a fixed, obligatory clause at the bottom of the e-mail that clearly informs that this e-mail could be viewed or controlled for archiving purposes. This is still no solution for those e-mails that one receives and that are still records that need to be stored.

Directive 97/66/EC is currently being reviewed in the light of the adaptation of the current rules regarding new and foreseen developments in the field of electronic communication services and technologies. The European Commission's aim is to make the Directive 97/66/EC technology-neutral via the new proposal[44]. To achieve this, a number of terms are clearly defined in the draft Directive, for example "traffic data". In the current Directive 97/66/EC Article 6 about personal data only applies to "calls", strictly interpreted only referring to so-called circuit linked connections (such as traditional speech telephony) but not to package linked transmission (such as use of the Internet). It is not technology-neutral to protect traffic data that stems from the set-up of a traditional telephone call but not the similar data that stems from the process of Internet communication such as e-mail. When introducing the definition of "traffic data" the European Commission considered it necessary to also protect the

[43] Official Journal, L 24, 30 January 1998, 1, http://europa.eu.int/eur-lex/en/pri/en/oj/dat/1998/1_024/1_02419980130en00010008.pdf

[44] Common point of view regarding the draft Directive concerning the processing of personal data and the privacy protection in the sector of electronic communication, 21 January 2002.

confidentiality of this data, next to the confidentiality of the content of the message. The proposed Article 5 now goes as follows:

> ARTICLE 5: CONFIDENTIALITY OF COMMUNICATION
>
> 1. The Member States shall ensure the confidentiality of communications and *related traffic data* by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, *storage*, or other kinds of interception or surveillance of communication and related traffic data, by persons other than users, without the consent of the users concerned, except when legally authorised to do so, in accordance with Article 15(1). This paragraph shall not prevent technical storage that is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.
>
> 2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.
>
> (…)

When this draft Directive is approved a gap will occur in national legislation regarding the protection of the principle of confidentiality of mail, in that sense that according to the draft Directive the protection of electronic communication also applies to *traffic data* related to the electronic communication. Traffic data is defined as any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof[45]. The principle of confidentiality of mail on the other hand traditionally only applies to the content of the letter; learning of its existence and even registering it is allowed, as long as the letter remains unopened and as long as the rules concerning the processing of personal data are applied[46]. By consequence also logging incoming an outgoing mails is only allowed with the explicit authorisation of those involved, as the server log files are traffic data. Logging implies that files are set up that contain information such as the date and time of sending, the sender(s), the addressee(s) and the file size of the incoming and outgoing e-mails and possible attachments.

Member states are allowed however to introduce exceptions to the principle of confidentiality of (the content of) tele communication by determining that telecommunication messages and traffic data must be stored by the service providers for a limited time. This is for reasons of national security such as preventing, investigating, locating and prosecuting penal offences committed via the Internet or unauthorised usage of the electronic communication system. The draft Directive also permits the technical storage of or access to electronic communication with as an exclusive goal to execute or

[45] Article 2 (b) of the draft Directive

[46] See below

facilitate the sending of correspondence over an electronic communication network[47]. The argument of technical supervision however only rarely applies to the employer, represented by the archivist, the records manager or the system manager wanting to scan the e-mail traffic on its archive value.

The Directive however wants to meet the concrete needs that occur in business traffic and poses that the principle of secrecy of telecommunication does not interfere with national legislation that allows registration of communication and related personal data as far as this is executed in legal business traffic to form evidence of a commercial transaction or of another means of business communication[48]. Business communication encompasses all non-personal communication. This Directive stipulation can therefore not be explained as making a difference between the public and the private sector. This stipulation allows Member States to introduce an exception to the secrecy of telecommunication principle in their national legislation regarding the execution of employers' surveillance to business communication performed within the organisation. Controlling e-mail usage by the employer usually focuses on that type of usage that endangers the efficient execution of the labour agreement because of, for example, excessive use or forwarding of classified company information. Archiving is a completely different problem: it does not focus on locating unauthorised usage of the medium as such but on the importance to the company of authorised usage such as for evidence reasons. We believe that the national legislators should not forget the archiving issue, as he has also foreseen an exception to the principle of secrecy of telecommunication for reasons of employers' surveillance as stated in Article 5.2.

C. E-MAIL ARCHIVES: PROCESSING OF PERSONAL DATA

It is not only the principle of secrecy of telecommunication that causes legal questions and problems when archiving e-mail. Archiving e-mail also implies that a processing of personal data takes place in the sense of 95/46/EC concerning the protection of individuals with regards to the processing of personal data and the free movement of such data (Privacy Directive)[49]. The legal problem concerning the processing of personal data does not only occur when archiving e-mail. It is a widespread issue that every archivist or records manager meets when managing his or her (electronic) archive.

1. Applicability of the Privacy Directive

The Directive is applicable to the automated *processing* of *personal data* and to the non-automated processing of personal data that forms part of a filing system. A "filing system" is a structured set of personal data that is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. Thus paper archives also fall within the scope of the Directive for as far as they are structured in one way or another. "Personal data" is defined as any information related to an identified or (directly or indirectly) identifiable natural person ("data subject"). Legal persons are excluded. "Processing" is any operation or set of operations that is performed upon

47 Article 5.3 of the draft Directive

48 Article 5.2 of Directive 97/66/EC

49 Official Journal, L 281, 23 November 1995, 31, http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

personal data, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available otherwise, alignment or combination, blocking, erasure or destruction. All treatment a records manager or an archivist can apply to e-mails will be classified as "processing".

E-mails often contain personal data concerning a data object. The e-mail header for instance contains the sender's and the recipient's e-mail address. An e-mail address is often information related to an identified or identifiable natural person. To be qualified as personal data the e-mail address does not need to lead immediately to the identification of a natural person. Whether a person is labelled as identifiable is based on all means available to the responsible of the processing or any other person to do the identification. For example one often receives an e-mail address when signing up with an Internet Service Provider to access the Internet. Also private companies that are not functioning as ISP sometimes offer on their website an e-mail service that provides free e-mail addresses[50]. The end user must fill in a form to make his personal data available. This allows the e-mail service provider to identify its users. This already suffices to be qualified as personal data.

Not all e-mail addresses consist of personal data though. An organisation's general e-mail address, often shaped similar to info@domainname, does not consist of personal data due to the lack of an identifiable natural person. The content of the electronic message usually contains additional data that allows the identification of a natural person next to the e-mail address, such as an automated signature message or a digital signature, accompanied by a certificate. This certificate allows the e-mail receiver to identify its sender.

When incoming and outgoing e-mails are registered and stored in the electronic mailbox of an employee, processing in the sense of the Privacy Directive takes place. This implies that some rules need to be lived up to, rules that the European Member States have transposed into national legislation. In this report we are discussing the provisions of the Directive, which are considered to be sufficiently clear, precise and unconditional. They are immediately effective whether transposed or not. The Directive however does not apply when a natural person processes e-mails containing personal data for personal or domestic goals. E-mails in the user's personal mailbox are therefore not subject to this Directive even if they contain personal data.

2. Who needs to live up to the rules?

The body responsible for the processing (the controller) has to supervise the compliance with the rules of the Directive. The controller is defined as: "the natural or legal person, public authority, agency or any other body who alone or together with others determines the purposes and means of the processing of personal data." It will not always be clear who is responsible for the processing of e-mails in an e-mail system. It will largely depend on who determines the goal of and the means for the processing. The body

[50] Microsoft's Hotmail service for instance has become tremendously popular. It allows its users to check their e-mail from most web browsers (http://www.hotmail.com).

responsible for the processing will always be the employer in those cases that an e-mail policy exists within the organisation that clearly determines what e-mail programmes needs to be used, to what ends it can be used, how e-mails need to be signed, if and what e-mails need to be stored during a defined period to ensure the proper functioning of the organisation, who is responsible within the organisation to solve technical problems, etc. However, if the employer only gives an e-mail address to his employees and if they are fully responsible themselves for what happens with it, it is the employee who is responsible for the processing. In any case it is a factual matter, but one that the employer has to look into. Most national legislation will punish controllers that do not comply with the rules.

The Data Protection Commissioner in the United Kingdom has composed a number of criteria to determine whether an organisation that manages an e-mail system can be defined as a data controller. The e-mails processed or stored within its system must [51]:

- Identify living individuals, and
- Be held in automated form in live, archive or back-up systems, or have been deleted from the live system but are still able to be recovered, or
- Be stored as prints in relevant filing systems (that is: non-automated or "manual" systems, organised according to criteria related to individuals and allowing ready access to specific parts of the information).

3. What rules apply to the body responsible for the processing?

The Directive starts from the point of view that the body responsible for the processing can only process personal data if one or more criteria apply. For each processing of personal data such as storing it, the archivist needs to determine what acceptability criterion applies. Any processing not based on one of the principles set out in Article 7 of the Privacy Directive cannot be performed. These principles are: unambiguous consent, processing necessary for the performance of a contract, processing for legal obligations, processing for vital interest or processing for public interest.

Regarding the processing of e-mails the principle may apply that the data subject has implicitly given his or her permission for the processing of the personal data that may appear in e-mail he sends. One realises that sending an e-mail implies that it will end up in a mailbox and that it might be stored there for some period of time. The main problem of archiving e-mail is not related to a possible prohibition of processing. However Article 6 of the Directive might cause problems, as it determines that personal data cannot be processed in a way that is incompatible with the goal for which the data was originally received (Article 6e of the Directive).

[51] *Subject access to personal data contained in e-mails*, Data Protection Commissioner, Compliance advice, 14 June 2000, http://www.dataprotection.gov.uk/dpr/dpdoc.nsf

4. Archiving: secondary processing complying with the original goal?

Archiving e-mail is a new and secondary processing of personal data. A 'secondary' processing of personal data can be any processing for a goal other than the one for which the data was originally collected. Collecting e-mails of the staff of an organisation by the records manager for the purpose of storing these e-mails can be qualified as a secondary processing. The Directive determines that a secondary processing of personal data *for historical purposes* could comply with the original primary goal (and is therefore allowed), as far as the Member States offer suitable guarantees (Article 6.1.b of the Directive).

Article 6.1.b) of the Directive has caused quite some uproar in the Belgian archive world because of the royal decree the Belgian legislator has attributed to it. The starting point of the "suitable guarantees" for the processing of personal data for historical purposes is a gradual three-step system that can be found in the royal decree of the Belgian Privacy Act of 8 December 1992[52]. As a principle the historical processing should take place based on anonymous data. If the historical purposes of the processing cannot be achieved by the processing of anonymous data, the controller is allowed to process coded personal data. And if this method still does not allow achieving the historical purposes, only then can the personal data be processed in its original form.

When this regulation was introduced the question arose within the archive world regarding the meaning of the term 'historical purposes'. Is the storage by an archivist of an organisation's proper documents an act of processing for historical purposes? If the answer is yes, the three-step system applies and an archivist needs to make all personal data anonymous before archiving it. Even though it is much easier to make data anonymous in a digital context than would be the case for paper data, this method would be unworkable for the archivist and furthermore it would be impossible to store e-mails in their original form.

Neither the text nor the considerations of the Directive contain a definition of the term "historical". In general linguistics the term "historical" refers to the processing of personal data with the purpose of analysis of a past event or the enabling of that analysis. Thus interpreted also an organisation's archiving of its proper cases would fall under the new arrangement. However we feel that "processing for historical purposes" in the Directive is meant as "the secondary processing for historical purposes *by another person than the controller*". Put differently: only when another person than the one responsible for the primary processing handles the personal data for a secondary, historical goal, for example a genealogist, the "suitable guarantees" of the Member States apply. On the contrary, the processing of the proper e-mails for archiving purposes is always in compliance with the original goal and can take place without obstacle.

[52] Modified by the Act of 11 December 1998 to transpose the Privacy Directive, Official Journal (*Belgisch Staatsblad*) 3 February 1999

D. CONCLUSION

The necessity to archive e-mails will hopefully be clear to the reader of this report. However, it will also be clear that quite some legal issues related to privacy are involved as well. The principle of secrecy of communication is a strictly formulated constitutional right. Furthermore the E.C.H.R. strictly sticks to it in its jurisdiction. As a principle it is forbidden to view the content of e-mails, to copy the content of an employee's electronic mailbox, even to check or register the main components of the e-mail such as its sender or its addressee, its subject, its priority, etc. This is even so if the content of the message is not viewed and also if the records manager of the organisation performs these actions to avoid the possible deletion of e-mails with archive value.

In real life this principle is applied with more flexibility. No organisation will ask permission of all correspondents involved to register incoming and outgoing e-mails. This method would be too time consuming and is often impossible to perform for some e-mails.

As it is common practice to view e-mails within an organisation, usually to detect unauthorised usage of e-mail by employees, it will be clear that the current principle of secrecy of telecommunication in its present wording is much too restrictive and does not comply with everyday needs. The Belgian Commission for the Protection of Privacy has pointed this out in its advice about the enactment to protect the citizens' privacy against overhearing, learning about and recording private communication and private telecommunication that transposes Directive 97/66/EC into Belgian legislation[53]. In this advice the Commission expresses its worries about the scope of the prohibition that according to the used definitions could punish perfectly legal practices. The example the Commission gives is the habit of many companies and governments to use an automated telephone switchboard to record certain characteristics of internal and external communication: number of the caller or the called number, date, time and duration of the call. The Commission is of the opinion that this should be made possible to prevent staff abuse. This reasoning however should also be valid for the archiving of telecommunication that is automatically registered (such as electronic mail messages) which turns them into records.

The Commission believes that applying the privacy legislation without questioning its validity will reduce the risk that stems from still registering telecommunication in those cases where everyday practice requires it. The three main principles of the privacy legislation are finality, proportionality and permission. They are the deciding factors, as it were, regarding every privacy matter.

One can wonder whether the application of these principles puts the principle of secrecy of telecommunication out of action. Of course it does not. Only the (European) legislator can alter or abolish a previously installed Act or Directive. The Commission's reasoning still leaves the organisation with some means to register and archive e-mails at almost no risk while waiting for legislative initiatives in the Member States to arrange employer's supervision of electronic communication.

[53] Advice nr. 23/93, available on http://www.privacy.fgov.be

- The most legal solution is to leave the selection of the e-mails to be archived completely to the end user. He can decide autonomously what e-mails should be stored and will add them to the relevant case or will forward them immediately to the organisation's records manager. This is permitted because one is allowed to forward a received mail to somebody else. The end user was taking part in the communication and has the freedom to dispose of what can be called a 'legally made recording'. This solution is only viable however in small organisations.
- Larger organisations cannot leave this responsibility to the end user. Their e-mail policy needs to look into the archiving of electronic mail to arrange this process in a proper way. The policy needs to determine what types of e-mail will be considered as records with archive value. This is best illustrated by some examples.
- If an organisation wants to view and register e-mails anyway for example because the selection by the end user is too time consuming or inadequate, the prevailing principle should be the 'reasonable expectation of privacy'[54]. This is always a matter of balancing between the employee's privacy and the importance for the organisation to possess a reasonable archive. The e-mail policy needs to indicate clearly what privacy expectation the end user can have regarding his or her e-mail within the organisation, taking into account the principle of secrecy of telecommunication and the privacy legislation as much as possible. This way it is clear in advance in what cases the principle of secrecy of telecommunication can be considered to be violated against or not.

  * To ensure that the finality of e-mail registration is not exceeded, the e-mail policy needs to determine that all e-mail in the employee's electronic mailbox will be considered as professional e-mail. Then private usage cannot be called in as an argument not to register the e-mail. The 'separation' of professional mail by taking these measures will not provide authorisation for the records manager to register and view the e-mail but it will limit his or her risk to be confronted with a complaint for violating the principle of secrecy of telecommunication.

  * Another possible measure can be to explicitly mention on each e-mail sent from the work place that it is a professional mail, and that each e-mail sent to the professional address can be viewed by the organisation (for example using a fixed text that is added as signature or by the usage of a 'company template'). Correspondents who later send e-mails to this address are then supposed to consent in silence. It is best to let the end user sign a paper in which he authorises the viewing or registering of e-mail. However there are no ways to protect the privacy of those who voluntarily send an e-mail to someone within the organisation. Extra caution will be necessary.

  * Verification by the records manager should always take place while keeping in mind the principle of proportionality according to Article 8 E.V.R.M. and the privacy legislation. This implies that the records manager can only perform those actions that are necessary to achieve an efficient archiving and only as far as they are necessary, even if he or she has received the necessary end user's authorisation and supposedly also that of the other correspondents. He or

[54] See the advice of the Dutch Registration Chamber of 24 June 1999, nr. 99.V.0141, available on http://www.registratiekamer.nl/bis/top_1_6_2_35.html

she cannot view the e-mails if studying the data related to the communication (such as sender and subject) suffices. He or she cannot continue reading the mail if it becomes clear immediately that the mail does not qualify for storage (for example if a mail would be found in the employee's electronic mailbox for which the subject itself already indicates that it is not a record).

- Finally organisations need to see that not only the end user's expectations need to be determined but also that this policy has to be made public within the organisation. Good organisational transparency can be achieved for example by publishing the e-mail policy on the start screen of the organisation's intranet.

V. OTHER RELEVANT REGULATIONS

A. INTRODUCTION

The government in particular has more than the privacy regulations to comply with. Looking only at the privacy legislation would make the storage of e-mail a long-term problem that only needs to be reflected upon after the e-mails have lost their immediate use to the government. Public authorities however need to comply with legislation regarding access to documents held by public authorities too. An e-mail addressed to or sent by the government can form a governing document in the sense of the legislation regarding access to governing documents. These e-mails must be kept available at all times to the citizen who asks for them. Governments need to be able not only to keep their e-mails available to the archivist. Also a short-term policy needs to be conducted for the dynamic and semi-static e-mail archive in order to respect the legislation regarding access to governing documents. It goes without saying that the archivist will play an important role during the composition of this policy.

B. ACCESS RIGHT TO GOVERNING E-MAILS

Twelve out of fifteen EU Member States have adopted legislation on access to governing documents[55]. This legislation seems to have no limitation on the type of carrier on which information can be held. Governments must indeed be aware that electronic information also falls under the application domain of this legislation. Swedish legislation defines a record as "any written matter, picture, or record, which can

[55] There is no general legislation concerning access to documents in Luxembourg, in Austria nor at federal level in Germany, where access to government documents is in principle only given to participants during administrative procedures. Special provisions providing a general right to access to documents are included in the constitutions of some Länder. (Status: October 2000; see *Comparative analysis of the Member States' legislation concerning the access to documents*, European Commission, http://europa.eu.int/comm/secretariat_general/sgc/acc_doc/docs/compa_en.pdf).

be read, listened to, or otherwise comprehended only by means of technical aids." In Spain a document may take a graphical, sonar or visual form or it can have any other material support.

No EU Member State legislation explicitly mentions e-mail as a governing document. Still public authorities must be aware that the right to access governing documents in many cases extends to e-mails and their attachments. In the U.S. the Freedom of Information Act Manual, a guideline for civil servants of the U.S. National Labor Relations Board concerning publication of public records, determines that all documents, including e-mail and documents created using a word processor, can be subject to publicity and need to be considered when a request for publication is being treated[56].

Rules regarding the publicity of documents of the European Institutions can be found in Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 concerning public access to European Parliament, Council and Commission documents[57]. This text does not clearly qualify electronic mail as a governing document either. Yet the European Institutions need to compose an e-mail archiving policy so that e-mail can also be considered for a request to access the documents in a certain case. For the purpose of the regulation, a document can be defined as "any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audio-visual recording) concerning a matter related to the policies, activities and decisions falling within the institution's sphere of responsibility".

It is therefore a principle that all information is public that can be found in the e-mails and attachments that a public authority possesses (except for Austria and Luxembourg). When a person requests a public authority for access to the documents in a certain case, one must take into account that this also applies to the relevant e-mails. It goes without saying that e-mails need to be carefully stored for this reason. Despite the lack of rules for the storage or deletion of official documents in the legislation in the Member States concerning access to governing documents, this legislation indirectly imposes quite some limitations that prohibit the destruction of official documents including e-mails. It is much less necessary here to work with the original electronic version than it is when archiving in the strict sense.

[56] Freedom of Information Act Manual, 8, http://nlrb.gov:foia/submanl.html

[57] Official Journal of the European Communities, L145/43, 31 May 2001

VI. ARCHIVING E-MAIL: THE OPTIONS

A. THE ARCHIVIST'S CHALLENGES

Despite the fact that e-mail has become part of everyday life, only few institutions possess a coherent recordkeeping strategy for their incoming or outgoing e-mails. This leads to situations where the administration is left alone, the administration archives prints at its own discretion or is even unaware of the possible archival value of e-mails. This is ending in parallel circuits that contain the same information in paper and electronic form, to illegitimate destructions, multiple copies of the same mail, stored e-mails in non-accessible off-line folders, etc. Nevertheless, the entirety e-mails and attachments represents a large part of an organisation's information and knowledge. After all, e-mail evolved from a informal to a standard office system and e-mails do not longer contain only ephemeral information but can play an important role in a work process. A clear and coherent recordkeeping strategy with clear procedures and guidelines for the organisation's e-mails can avoid this in the future and must lead to archiving and accessibility of e-mails with archival value. E-mail archiving is a challenge as it confronts archivists with the main questions that accompany the management of electronic records.

The archiving of e-mails requires a serious effort with regard to intellectual recordkeeping. The e-mail system is an information system that is not connected to the recordkeeping system for (electronic) records. For reasons of accessibility and interpretability the e-mail message needs to be linked to the structure and the context of the archive. The link between the e-mail message, the attachments, the other related records and the work process must be incorporated in the recordkeeping system one way or another. To allow later consultation and interpretation it must be clear in what work process the e-mails have been created or used and what their relation is with other related records. The importance of the archival bond should not be underestimated: it gives the document the status of a record[58]. Archiving the context is also relevant to help demonstrate the authenticity and reliability of records. While the archival bond is usually stored physically in a paper environment, this is only possible in a logical or intellectual way for electronic records[59]. The e-mail context is not contained in the sent or received message itself. Sender and addressee do know the context and need to establish it explic itly some way or another. Both paper and electronic recordkeeping will add the necessary contextual information to the messages at the time of creation or reception. The current e-mail systems however do not possess this functionality by default, so that the relation with the work process and other documents can only be stored using ad hoc solutions.

On the other hand the development of an archiving strategy needs to take the organisation's technological infrastructure into account. One organisation will have the possibility to purchase an additional computer application for e-mail archiving, while another will only possess a standard e-mail

[58] L. DURANTI, *The archival bond*, p. 216

[59] T. THOMASSEN, *Een korte introductie in de archivistiek*, p. 14-16

software package. In the latter case the big issue will be to incorporate e-mail recordkeeping functionalities into the existing e-mail software. Also within one organisation there is not always a homogeneous technological infrastructure available so that different situations can occur. Not every department of the same institution will use the same document management system or e-mail software package.

Archiving e-mails is a fine example of the principle of *records continuum*[60]. Due to the need of selection, creation of well-formed e-mails and explicit contextualising one is obliged to start the archiving process the moment the e-mail has been created or received. The archivist is obliged to act as records manager and to jump into the administration with the recordkeeping system.

Due to the amount of e-mails it is better for archiving to take place in an automated way. In the Belgian context, interference of sender or addressee can't be completely avoided for juridical reasons. However, human interference should be reduced to a minimum. An additional obstacle with regard to this given is the lack of any tradition of records managers in Belgian or Flemish government. The administrative assistants are in charge of their own records management. On the other hand, selection should also be allowed, as there is no need to store e-mails without archival value.

Finally e-mails need to be archived in a sustainable and durableway, guaranteeing their authenticity and integrity as well. Those e-mails with archival value should be stored with as many guarantees as possible regarding long-term legibility.

There are many challenges to archivists. The e-mail recordkeeping system needs to offer solutions to each one of these challenges.

B. QUALITY REQUIREMENTS FOR ARCHIVING E-MAIL

E-mails with archival value must be considered as electronic records. E-mail record keeping needs to comply to the quality requirements that are applicable for electronic records in general. Applied to e-mails, this means that archiving e-mail messages complies with the following demands:

- The archived e-mail messages are complete. Their content, structure and context are to be archived[61].
  - *content*: next to the actual message, an archived e-mail also contains all the essential transmission data. This consists of the name of the sender, the name(s) of the addressee(s), the subject, the recipients of the copy/copies, the date and

[60] S. FLYNN, *The records continuum model in context and its implications for Archival Practice*, in: *Journal of the Society of Archivists*, vol. 22, nr. 1, 2001, p. 79-93

[61] *Guide for managing electronic records from an archival perspective*, p. 10; K. THIBODEAU, *Preservation and migration of electronic records: the state of the issue* (http://www.nara.gov.au). The structure of a record is the relation between its composing elements. The context of an record is the archival link with all related documents.

time of sending and reception. If one of these is missing the message is not complete. Attachments are also incorporated into the content of the e-mail.

- ? *structure*: the relation between the elements that compose an e-mail will be archived. An e-mail's fixed elements are a header, a body containing the actual message and the possible attachment(s).
- ? *context*: e-mails will be archived within their context. A reference to the work process in which the message has been created, received or used will be archived together with the e-mail. Also the link between the e-mail and related documents such as attachments should be clear when consulting afterwards[62].

- The content, transmission and contextual data of each e-mail are inseparably linked to each other. All these elements and their links have to be (electronicly) archived in a durable, persistent and platform independent way.
- The e-mails with archive value will be incorporated into the organisation's recordkeeping system. This system is secured and will prevent modifications or manipulations to the archived e-mails. The archive system helps to ensure the authenticity and the reliability of archived e-mails. The archived e-mails will be authentic and correct.
- The archived e-mails are readable in the long term. The e-mails are stored in a suitable file format. The file format will be sustainable, legible and user friendly.
- The archived e-mails are accessible. The (computer) system that manages the archived e-mails must be able to retrieve them based on their content, header data and context.

C. THE E-MAIL ARCHIVING STRATEGIES

There are several ways to archive e-mails, and this section will discuss all of them. Each option will be checked according to predetermined quality demands.

1. Hard copy recordkeeping

Applying the hard copy option implies printing the e-mails and storing them on paper, microfilm or microfiche. As a consequence e-mails are not stored in their primary form but are being replaced by prints on paper or microfilm/microfiche. Replacing the original electronic e-mails also results in the loss of the advantages of electronic information: more storage space in the repository is needed, the e-mails can only be consulted at one location, simultaneous usage is impossible and the archived e-mails cannot be quickly searched, sorted or indexed.

[62] The obligation to mention this data is Among others embodied in the American DoD 5015.2 standard (see C2.2.3: Filing Electronic Mail Messages).

Yet the hard copy option can have some importance to the archiving of e-mails. The widespread commercial e-mail systems do not fulfil the recordkeeping needs. Electronic e-mail recordkeeping often requires a customised solution that can be technically so complex that no off-the-shelf products can be used and/or that the price will be high. The National Archivist of the United States argued in the GRS20 case that the decentralised storage of e-mails in personal mailboxes or on different workstations definitely does not meet the demands concerning structured and accessible storage. Hard copy archiving complies easier with these demands, which justifies incorporation into a paper recordkeeping system. Paper archiving has some indirect additional advantages: the message is being transposed onto a more durable medium and the long-term problems of file format and readability are avoided.

However the main argument in favour of hard copy archiving is the lack of an efficient electronic recordkeeping system. It is better to archive on paper in a good, structured and accessible way than to preserve electronicly in a bad way[63]. Administrations with a predominant paper recordkeeping system can thus also avoid a hybrid information system. One needs to use this last argument with great care though. Information is more and more present in electronic form. The choice for a paper recordkeeping system for e-mails could imply that in the long run both a paper (for e-mails) and an electronic information (for other records) system will be present so that the organisation has nevertheless a hybrid information system. It should be said that paper archiving is only to be considered as a short-term solution while waiting for a recordkeeping system for electronic records. When this becomes available a changeover to an electronic e-mail recordkeeping should be made. While such a system is being developed and implemented, e-mails can be archived on paper.

It is relatively easy to develop a decent paper recordkeeping system for e-mails. Similar to classical paper correspondence the necessary registration data can be put on the print. Adding the printed e-mail to the file related to the subject or the case will store the message together with the other related documents that have been created in the same context. This results in a physical storage of the archival bond. However this does not apply when the archived e-mails are put on microfilm in one large series. The attachments to e-mails can be printed and stored in the same case or subject file, even though not all types of attachments can be printed (sound, moving images). Until today many institutions use this recordkeeping strategy. They do not yet possess an recordkeeping system for electronic records and therefore extend their recordkeeping system for paper records to e-mails.

Some points require consideration before this archiving strategy can be applied. Firstly there is the quality requirement that printed e-mail needs to contain all content and transmission data. The e-mail systems contain a number of standard layout templates for printing e-mails. These templates determine which header data needs to be printed. Not all required fields are automatically printed. In general only the data on the screen is printed. For example the *memo style* of MS Outlook does not print the date and time of reception by default. This does happen in the *table style* but here the date and time of sending are missing. However both dates and times are present within the e-mail system for each e-mail. The print

[63] In this case the paper storage of e-mails is a valid option in for example Australia, the United States and the Netherlands (Australia: http://www.naa.gov.au/recordkeeping/er/elec_messages/policy.html; US: GRS20 case; the Netherlands: HORSMAN P., *Archivering van elektronische post. Methoden, meningen en alternatieven*, p. 15).

style or the form for incoming e-mails may therefore need some modification (see further)[64]. The data related to the archival bond can thus be added to the e-mail message or can be added manually with a stamp on the print.

Filip Boudrez

From:	Filip Boudrez
Sent:	Thursday, August 19th 2002 10:31
To:	Willem Vanneste
Received:	Thursday, August 19th 2002 10:31:13
CC:	david@stad.antwerpen.be
Subject	Archiving e-mail

Image 1: Example of an e-mail header on paper where all transmission data has automatically been printed. This was made possible by adapting the e-mailheader for incoming e-mails.

Secondly hard copy archiving implies the destruction of the original electronic e-mails. This requires the authorisation of the Belgian General State Archivist or his/her deputy. If the electronic e-mails are not destroyed a parallel circuit will come into existence containing the same information. Electronic e-mails are not stored in a controlled environment and can no longer be used as evidence or proof of liability. To enable this there should thirdly be a clear procedure for e-mail printing so that also the authenticity and integrity of the paper messages can be assured.

2. Electronic recordkeeping

a) Archiving centrally via the mail server or by the involved administrative assistant?

Technically speaking it is perfectly possible to archive a copy of each incoming and outgoing e-mail directly on the mail server together (or not) with attachments. This would allow not a single e-mail to escape archiving and would relieve the administration from its active role in the recordkeeping process. The international literature presents this approach as a possible archiving strategy[65]. Peter Horsman

---

64 A United States lawsuit ruled in 1993 that the paper print of an e-mail is not necessarily identical to its digital version (*Armstrong vs. Executive Office of the President*, also referred to as the *PROFS case*). The print contains less data than the e-mail stored within the e-mail system. Storing the text of the message was not enough. Also the transmission data and the attachments form part of an e-mail message. The American government reacted to this judgement by forcing the administrations to ensure that prints contain all transmission data (http://www.gcn.com/archives/gcn/1998/_February9/gellm.htm). In the judgement of the Court of Appeal of 6 August 1999 the law seeking *Public Citizen* argued that paper prints are no identical substitutes of the original digital versions. Yet the GRS20 standard, a general selection list of NARA, number 14 stipulated explicitly that paper or microfilm archiving must ensure that this data is transported as well outside of the e-mail system. Despite the preference for digital archiving of the NARA and the Court of Appeal, the judgement of 6 August 1999 determined that digital archiving cannot be made obligatory and that adequate paper versions can replace digital originals.

65 For example STATE RECORDS NEW SOUTH WALES, *Managing the message-Guidelines on managing electronic messages as records. 5. Capturing electronic messages into recordkeeping systems*. In the U.S. the PROFS and

contemplates in his guiding brochure whether such a collection of e-mails would have a great future value. Such a collection may contain information that does not appear in other documents or can reflect the usage of this medium, which may be important to reconstruct the actions of an organisation[66].

Archiving directly on the mail server is met by some legal and archival obstructions however. An archivist would indicate that such a bulk collection would contain much e-mail without any archival value. Appraisal and selection is necessary because of the accessibility and the cost. Keeping everything is unsustainable in the long term. Preserving the context by linking e-mails to the organisations functions or activities would cause troubles too if this option would be applied. A context reference could be added to sent e-mails, but received e-mails would have to be archived without their archival bond.

Archiving directly on the mail server is in Belgium legally identical to intercepting an e-mail during its transfer. This is only permitted if one possesses the explicit authorisation of sender and addressee. If not one commits a penal crime. It is practically impossible to possess this authorisations for each e-mail[67].

From a legal and archival point of view the options for electronic recordkeeping are limited to archiving that involves the interference of the sender or the addressee. On the one hand this offers an extra value. The sender or addressee is best acquainted with the content or the function of messages. Both factors matter to distinguish e-mails with the status of record from those without this status[68]. The sender or addressee is also expected to put the e-mail in its context and to attribute a reference which reflects the archival bond. The consequence is however that this archiving process will only succeed if the administrative assistants apply it properly. Coaching and schooling of the administration will be important to make the archiving successful.

b) Electronic archiving within the e-mail system?

Whether e-mails can be preserved within the e-mailsystem, will depend largely on to what extent e-mailsystems can meet the quality requirements. A first condition for proper electronic recordkeeping is that e-mails need to be archived in the context in which they were sent, received or used. E-mails without context are not accessible or interpretable. This can be achieved in two ways in an electronic environment: storing the e-mails within a logical folder structure and/or adding a case number or classification code to each e-mail.

GRS20 cases made it clear that employees have no privacy rights when sending or receiving e-mails via the e-mail system that their employer has put at their disposal.

66 P. HORSMAN, *Archiveren van elektronische post*, p. 12

67 See the section on telecommunication secrecy in the first part of this report and the article S. VAN DEN EYNDE, *Archiveren van e-mail. Deel 1: Controlerechten van de records manager*, in: *Bibliotheek- & Archiefgids*, 77 (2001) 5, p 15-19.

68 In an attempt to solve this, an old version of the Australian Directive suggested that the sender should determine whether or not the e-mail is an archive record before sending it. This should allow computer selection based on the status of the messages. However this is only useful for the sender and does not offer a solution to the addressee.

Storing computer files within a logical folder structure is the most common method to group related electronic records and to add some context to the e-mails. Most current e-mail programmes allow e-mails to be stored in on-line and off-line folders. Sent and received e-mails are normally stored in the personal mailbox on the mail server disk. This personal mailbox is placed in a secured folder on the mail server disk with access limitations imposed by a user account and a password. Sent and received e-mails can be relocated from this personal mailbox to on-line and off-line folders. The on-line folders are placed on the mail server's hard disk and are accessible to everyone with access rights. A public folder can thus be made for an entire department or for all staff working on the same project. The off-line folders (for example *.pst files or *.nsf files) are best stored on a hard disk that is not part of the mail server. This could be another server disk or a local hard disk. The e-mail client programme allows the management of e-mails in on-line and off-line folders. Both types of folders contain the messages and their attachments. This implies that they can grow to a considerable file size quite quickly. Many network managers have determined a maximum file size for the personal mailboxes and on-line folders. E-mail users therefore need to clean their mailbox on a regular basis. Not to overload the mail server, preference is given to off-line storage of e-mails with archival value as much as possible. All folders and e-mails placed in one off-line folder compose one big computer file (for example MS Outlook: *.pst files; Lotus Notes: *.nsf files). The disadvantage of this off-line folders is that they can't be easily shared.

Similar to a hard disk the on-line or off-line folder can receive a structure within which the e-mails with archival value are stored. The development of such a folder structure allows an arrangement based on functions or activities. As the function of the archive is to document and prove the work processes, this target is best realised when the folder structure reflects those work processes and more specifically the functions, tasks and activities of the creator. By preference this folder structure is hierarchical and arranged from general to specific. The general functions of the creator make up the main sections. For each task or activity a subfolder is created within those main sections. If desired these folders can be further subdivided per subtask or subactivity. The lowest level holds a folder containing the e-mails for each dossier, file or subject[69]. The folder structure then reflects the logical structure of the archive and the context of the archive components.

[69] Such a structure is close to a classification scheme or filing plan. Most operating systems or applications sort the folders alphabetically on name, so that the folder order does not reflect the classical order of the functions (internal ? external, general ? specific). This can be avoided by adding a code to the foldernames.

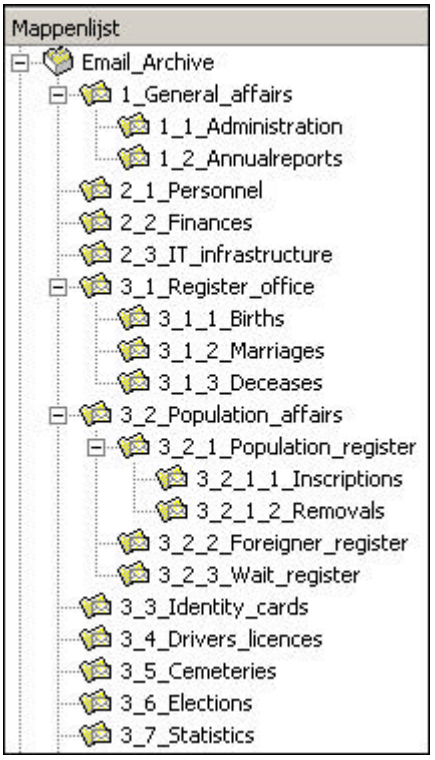


Image 2:
A folder structure for a Population Register Department within the e-mail system. The whole department possesses a hierarchical folder structure within one public folder. The different tasks of the department form the main sections. These are further subdivided in subtasks and subactivities. The lowest level contains a separate folder for each case or subject.
The foldernames are preceeded by a code so that internal and external functions aren't mixed. This code can be used to make a reference to a file or subject.

The end result should be a logical and clear folder structure that already situates each e-mail partially in its archive context. Confusion, unclearness and multiple folders for one message should be avoided at all times. Some rules need to be applied when developing and applying a decent folder structure within the organisation[70]. These rules can relate to:

- The folder names: folder names must be unique, clear and semantic (self-descriptive). Abbreviations need to be clear to every person within the organisation.
- The creation of new folders: the main structure should be fixed and can only be adapted by the system manager in agreement with the records manager or archivist. Administrative assistants can only add folders on file or subject level.
- The tuning of the folder structure on the shared served disk to the e-mail system and possibly the paper classification: using an identical folder structure will allow integration of all related paper and electronic records.
- The use of a classificationcode which can be used for references. Classificationcodes avoid the problem of alphabetical sorting of folders on their names, reflect the structure and can be used to establish the archival bond.

Grouping electronic records in a folder structure is important for several reasons. Firstly, the records which belong together are grouped in one logical entity. Secondly, it allows the management of records at file level. Management decisions regarding to appraisal, disposition, preservation and access will be made at folder level. This will save time in comparison with managing the records one by one. Thirdly, a

[70] The website of the Antwerp City Archives contains guidelines for the development of a folder structure (http://stadsarchief.antwerpen.be → Werking archieftoezicht → Archiefbeheer → Digitale Archivering).

well structured folder structure gives the user access to the records it contains. By browsing the structure, it must be possible to find the records one need. Fourthly, the structure provides information about the context. Finally, the folder structure will often also reflect the structure of the paper archive, which is important for the integration of paper and electronic records.

Another possibility to link e-mails to their context is adding a case number or classification code to them. Adding this information to an e-mail stores the archival bond with the context. The standard e-mail systems however have no fields foreseen for this in the sefault headers[71]. Common e-mail systems such as MS Outlook or Lotus Notes do contain the functionality to enable this. Adapting the templates for incoming and outgoing e-mails seems to be the most appropriate option for this. Extra fields are added to the templates that allow the sender and/or addressee to add a reference or link to the context. The same solution can be applied to establish an explicit link between e-mail and attachments. Extra fields can be foreseen in the standard e-mail header or body so that every incoming or outgoing e-mail provides the necessary space. This is an application of the *encapsulation principle* and links the metadata that indicates the archival bond to the e-mail message in a inseperable unit. This again implies that e-mails can be retrieved later based on this information (for example a case number). The templates for incoming and outgoing e-mails will be modified.

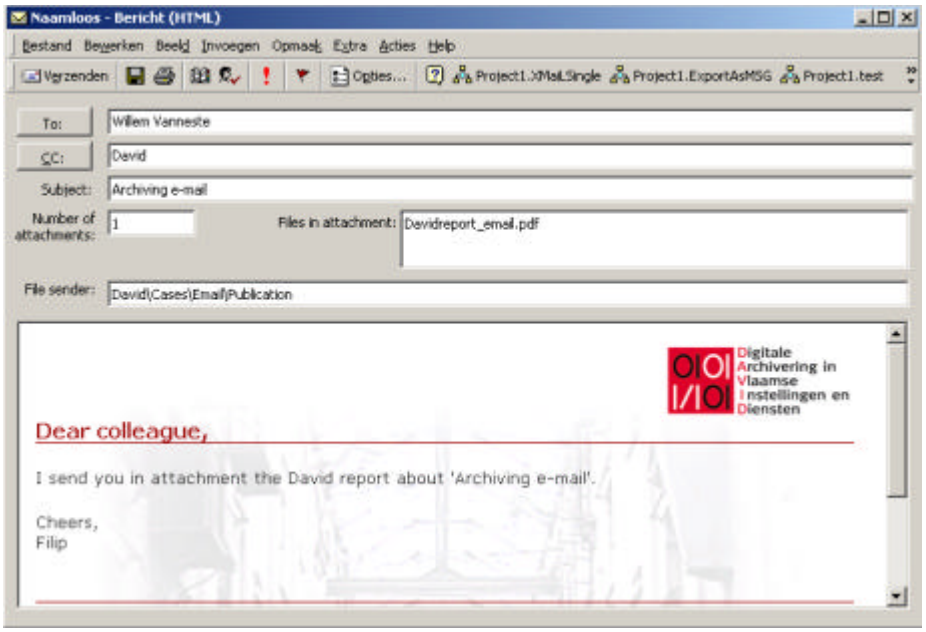


Image 3:
The necessary extra fields will be present in the header.

[71] Some authors have proposed to add this information to the "subject" field. However this would only work for the archiving of outgoing mails. This would imply that the original content of the "subject" field of incoming mails would be altered.

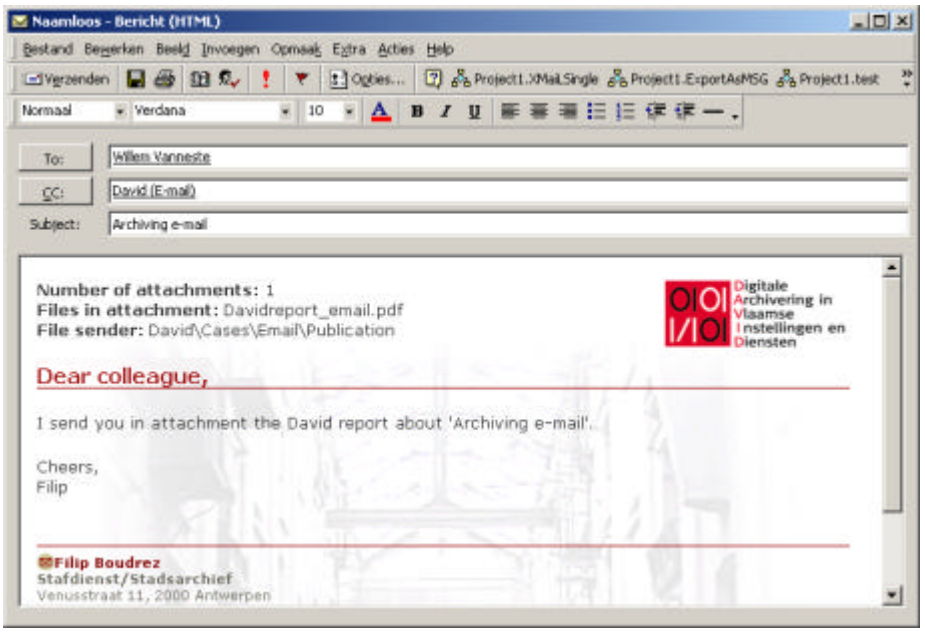


Image 4:
The body template will foresee three standard fields for the contextualisation of the e-mail. When opening concept these three fields are automatically mentioned in the body.

Next these templates are incorporated in the standard or corporate library of the mail server so that they are available to every person within the organisation. It seems to be best that the whole organisation shares the same templates and that these extended templates are installed as the default ones. This ensures that everyone creates well-structured e-mails that refer to their context. This will also allow the introduction of a house style for an organisation's e-mails. Filling-in the extra fields will be no more than an automatism such as filling in the fields 'our reference' and 'your reference' in a classical letterhead. In order to make this e-mailheaders user-friendly it is even possible to add some scripts which to automate the filling in of the additional fields.

The client mail programmes possess a number of search and sort options to allow an automated retrieval of archived e-mails. Furthermore the folder structure can be browsed as well.

Within the e-mailsystem a solution can be found for two essential requirements: contextualising and linking e-mails with attachments. However some important disadvantages are connected to this permanent storage of e-mails within the e-mail system that make this option insufficient for long-term archiving.

- E-mail systems are primarily information systems and not document management or recordkeeping systems. They do not possess the essential functionality for document management or recordkeeping (among others: description of context and work processes, disposition, etc.). Furthermore they are unrelated to the systems that do fulfil these functions. E-mails need to be stored within the recordkeeping system just as other records (for example letters or internal reports).
- E-mail systems have not been designed to group all related documents. Only the messages and their attachments related to the file or subject can be grouped within the e-mail system. Other documents that have not been composed or received via the e-mail system will not be incorporated to the folder within the e-mail system.

- E-mails are not stored in an accessible way in the archival sense. User names, passwords and access rights protect access to mailboxes and public folders. E-mails stored in folders with limited access or on local hard disks are of little use to the organisation or to researchers at a later stage. The archived e-mails will be spread over different folders and computer files.
- The e-mail systems are not capable of storing and centralising large amounts of e-mail. Long-term storage of e-mails within the e-mail system will cause storage problems and threatens the performance of the mail servers.
- The e-mails and folders will be stored in a software dependent format. The e-mails can only be viewed with a matching computer application. Each replacing or version update of the e-mail system may cause the need to convert or migrate all archived e-mails.

In brief, archiving within e-mail systems does not meet some important quality demands. E-mails with archival value can at most be temporarily stored within the e-mail system. The common e-mail systems are not suited as final storage environment for e-mails with record status. The same goes for back-ups of mailboxes on the mail server.

This does not imply however that e-mailsystems can't be used at all within the global recordkeeping process. Adjusted templates for incoming and outgoing e-mails help the creation of well-structured e-mails and allow the sender or addressee to refer to the attachments by filenames and to the context by means of an added case number or classification code. Storing the e-mails with archival value in the matching folders can already take place within the e-mail system. The recordkeeping process should not stop here however: the e-mails need to be transported outside the e-mail system and incorporated into a recordkeeping system. The preferences and possibilities of the organisation determine whether this archive system should be paper based or electronic.

c) Electronic archiving outside the e-mail system

If an electronic recordkeeping strategy has been selected, the e-mails need to be exported outside the e-mail system. A solution has to be found for the grouping of all related electronic records, for corporate access, for retrieval, for the preservation of large amounts and for software dependence.

To solve the readabilityproblem, the e-mails with record status must be migrated to a suitable file format for preservation purposes. Current e-mail systems possess a standard functionality to place e-mails outside the e-mail system. This functionality is called ‘archiving’ in MS Outlook and ‘exporting’ in Lotus Notes. E-mails can be exported individually or by folder. This last option is not ideal though: all e-mails will be exported sequentially into one single computer file. It is better to archive the e-mails as separate entities. The e-mail client programmes usually offer a standard choice between about five file formats: their proper format, Excel, Access, Lotus 1-2-3 or Unicode. The first four formats are not suited as archiving format due to the constant need of migration. Unicode offers more guarantees in the field of long-term legibility. Our preference however lies with XML (*eXtensible Mark-up Language*).

XML files are as sustainable as Unicode files and are very much suited to archive the content and the structure of an e-mail. XML best approaches the ideal of *Persistent Object Preservation*. The *Persistent Object Preservation* method is the object oriented archive strategy that the American San Diego Supercomputer Center is currently developing together with NARA for a complete electronic archive. The basis of this storage method is the idea that the current options for archiving of electronic records (storage of original hardware and software, migration, emulation) all have their weaknesses and are therefore insufficient or inefficient in the long run. The researchers want to store computer files in such a way that they will remain legible for 300 to 400 years without undergoing modifications. To achieve this the archived files need to comply with the following demands[72]:

- Storage in a technology neutral file format
- Accessible from future heterogeneous platforms without conversion or migration: this will reduce possible threats of authenticity and reliability violations to a minimum
- Be extensible and adaptable to future needs
- Be self-descriptive

The *Persistent Object Preservation* method starts from a selection of the elements that compose the record. All elements that classify a computer file as a record will be archived. It is generally agreed that the content, the structure and the context of a record are essential. In some cases the shape or appearance must be added to this.

The electronic records are stored as XML files. XML is platform independent, (semi-) self-descriptive, extensible, legible (after a minimal interference of software and hardware) and standardised. The structure of the records can be preserved via DTDs or XML Schemes. These formally define the selected elements and their relation[73]. By *parsing* the XML files the validity of the XML file structure is checked against the formal structure in the DTD or XML Scheme. This can be perfectly applied to e-mails. Within one organisation a fixed structure for the e-mails should be imposed (see template usage). This will mean that only one transformation procedure to XML files is necessary.

When the header data of an e-mail are stored as separate elements in the XML files, e-mails can easily be retrieved or sorted based on this. A second advantage is that the header data can be used as descriptive metadata when the e-mail is to be entered in the document management or recordkeeping system of the

---

[72] The NARA website (http://www.nara.gov.au) has multiple articles and presentations of K. Thibodeau available about the *Persistent Object Preservation* method (*Building the Electronic Records Management Information Infrastructure*; *Persistent Object Preservation: Advanced Computing Infrastructure for Digital Preservation; Preservation and migration of electronic records: the state of the issue*). The researchers of the San Diego Supercomputer Center have published articles about this storage method in D-Lib Magazine (*Collection-Based Persistent Digital Archives*, parts 1 and 2) and on their institution's website. It must be remembered regarding the predefined period of 300 to 400 years that XML files will only remain useful as long as computers can read Unicode characters. It is generally assumed however that Unicode will remain the basis for new character tables. When XML will become unused of lose its status of standard, the XML files do not need to be transposed: an adapted interface (for example a web browser) should do to read the files.

[73] The Antwerp City Archives applied this method when digitally archiving the digital voters' registers from 1994, 1995, 1999 and 2000 and information from the population records. The DAVID website contains more information about these cases. It was predefined what elements were to be archived. The electronic records were stored as XML files and their structure was fixed in accompanying DTDs.

archive department. This allows for an automatic description of e-mails. There are then multiple possibilities for the retrieval of e-mail: a structured query on the content of the e-mail headers, full-text queries on the content of the messages or a combination of both, etc.

Most e-mail messages do not contain any layout information and can therefore be stored as plain text files. Some mail client programmes allow layout of an e-mail message. HTML pages and style sheets are used for this. Client programmes that do not support this will view the e-mail message as plain text file. If the appearance needs to be archived as well, a style sheet can be added to the XML file. Another option consists of the *Multi-Valent Documents* that add a bitmap of the original document as a layer to the computer file. In general however, the lay-out of e-mails is not to be preserved.

Adobe's PDF (Portable Document Format) is a second file format that can be considered as archiving format for e-mails. Instead of a print on paper the e-mail message is copied onto a PDF file outside the e-mail system. The advantage of the PDF format is that the migration takes place in a quick and simple way. One only needs to possess the Acrobat software package that can be installed off-the-shelf. The Acrobat Distiller or Acrobat Writer will place the e-mails as separate PDF files outside the e-mail system. The latest PDF version (1.4) allows a structured data storage. The general disadvantage of PDF, from an archival point of view, is that it requires specific software for consulting, that it has the status of a vendor specific standard and that it does not base the storage of its characters on Unicode. HTML (HyperText Mark-up Language) could be considered as a third possibility, even though the archiving of pure text documents in HTML is not very common. HTML does have the status of an official standard however.

When deciding upon the archiving format the advantages and disadvantages of every format need to be measured. Compared to XML, e-mails stored as PDF or HTML files have some important disadvantages. PDF or HTML files only allow full text searches as automatic description based on header data is not possible. Archived e-mails in XML can also be searched or sorted based on their header information. Neither is the structure of the e-mails in PDF or HTML fixed in a formal way. Moreover, e-mails stored as XML-files can easily be transformed into PDF or HTML. The main disadvantage of XML is that it is not incorporated yet in the most recent versions of the common e-mail systems. This implies that the e-mail systems need to be adapted to allow an export as XML file. It is easier to store as a PDF or an HTML file. HTML storage is a standard feature in most e-mail systems, and PDF storage only requires Adobe's Acrobat. In any case it should be clear that XML, PDF and HTML are better options that storing e-mails in the system's proper file format.

After the exporting outside the e-mail system and the migration to a suitable archiving format took place, it is best to foresee a verification phase. One must be certain that the e-mails have not been altered during the migration and that no information has been lost. Ideally each migrated e-mail should be checked, but this will usually be impossible. Normally log files of the transposition procedure or random samples should do. XML files could be *parsed* against a DTD or even better an XML Scheme[74]. In both cases it is

[74] It could be a problem to find a suitable storage location for the DTD or the XML Scheme. In principle each e-mail stored as XML file can refer to the same DTD or XML Scheme. It is just that a suited location for this file needs to be found. This location must be everywhere accessible and should never change. Otherwise the path indication must be altered in each e-mail header. The Internet seems to be the most appropriate solution (for

the validity of the structure of the XML files that is being checked. An XML Scheme also allows a check of the type and number of characters. However this is not a real content control. *Parsing* for example will not show any content mix-up of the fields 'sender' and 'addressee'. As is the case for every migration, also the export outside the e-mail system and the transposition into an archiving format will need to be documented.

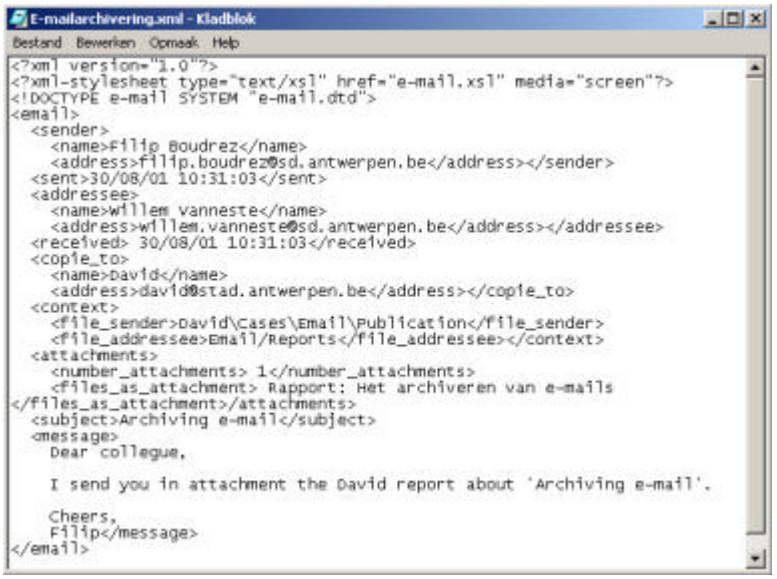


Image 5:
An e-mail stored as XML file. The header data or transmission and contextual information of the e-mail has been stored as separate elements. The archived e-mails can later be queried based on the content of these fields. This e-mail is linked to a style sheet. The structure of this e-mail is more elaborate than the standard structure in e-mail client programmes. The elaboration of the structure is a consequence of the adaptation of the headers in e-mail forms or templates (see further).

When e-mails are placed outside the e-mail system as separate files they also receive a file name. This is usually by default the content of the 'subject' field but this can be changed. It should be ensured that e-mails receive a unique file name. Otherwise, computer files with the same name that end up in the same folder will overwrite each other. A unique file name is also important to have the attachment link to the matching e-mail.

The e-mails are stored outside the e-mail system in a folder structure that forms part of the recordkeeping system. This folder structure should should correspond to the one within the e-mail system. Exported e-mails will appear as separate files in the same folder as in the e-mail system. The division into folders allows file formation and integration with the related electronic records which weren't part of the e-mailsystem. That is why it is important to adapt the folder structure within the e-mail system to the global folder structure of the shared workspace on the server disk. The moment the export outside the e-mail system of e-mails and attachments takes place, also the integration with other electronic records related to the same case or subject happens. All related records can be grouped this way: the internal electronic documents on the shared workspace, the e-mails and the received attachments. The result will be an electronic dossier which contains all related electronic records. Corporate access to the folders can easily be foreseen.

example immediately after the organisation's URL). Other options would be the common storage of DTD or XML Scheme in every folder (no path indication required, only a file name) or the use of an internal DTD.

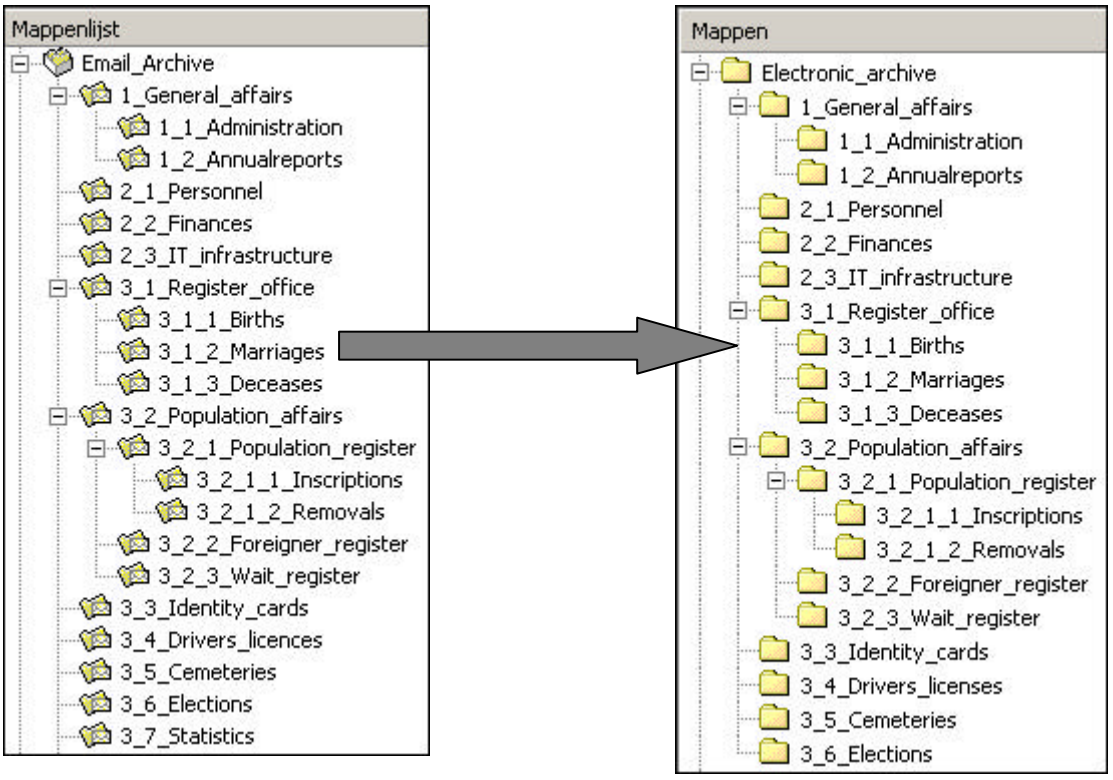


Image 6: The folder structure inside and outside the e-mail system should be compatible. When exporting outside the e-mail system the e-mails will end up in the same folder structure so that all related digital documents are grouped. Attachments can be placed in the external map immediately after reception or be exported at a later stage, together with the e-mail.

At the latest at the moment of the export outside the e-mail system there will be a separation of e-mail and attachment. The metadata of both electronic documents will keep the mutual reference so that the link remains intact. As for attachments the most suitable archiving strategy should be applied, based on the type of document. As attachments usually take up most storage space on the mail server, it can also be appropriate to export them outside the e-mail system immediately after reception. The attachments one sends oneself are usually already part of the shared storage space and are normally already placed in the corresponding folder.

To avoid unjustified altering, destruction or moving, the folder structure outside the e-mail system should be secured. This security should arrange an access control and protect against unjustified manipulations but it should also protect against viruses. Most mail servers will have an anti virus package installed but it is safer to perform a new virus check before adding the e-mails and their attachments to the digital repository.

It is best to assume the folder structure in the document management or recordkeeping system. The final step in the archiving process will then be the destruction of the e-mail versions within the e-mail system. From now on, the migrated e-mails will be the authentic versions.

3. Conclusion: archiving outside the e-mail system

The description and evaluation of the possible archiving strategies clearly demonstrates that e-mail messages can best be stored electronicly and outside the e-mail system. E-mails are printed and stored in the respective files (hard copy) or they will be stored in a folder structure outside the e-mail system in a suitable preservation format (XML, PDF, HTML). Both options have important consequences regarding the assurance of authenticity and reliability of the archived e-mail. In a digital environment the digital signature can be used to put a legally valid signature. A (digital) signature has three functions: identification of the sender, verification whether the content of both the sent and the received message is the same, and preventing the sender from denying that he or she has sent the message (non-repudiation) The digital signature can only be used as an alternative for a paper signature on the condition that the verification can be repeated at any given time after the archiving. The addressee can perform the verification at the moment of reception but this will no longer be possible after archiving based on the original digital signature. The hard copy option will even no longer have the digital version available. Digital archiving will have resulted in a migration of the e-mail message to another file format, and also the addressee will have added some registration data. The bitstreams – based on which the digital signature of the sender has been calculated – will be changed to such an extent that the sender's digital signature will no longer validate the archived e-mail. It is yet unclear how authenticity and integrity need to be guaranteed in this case. Further research is necessary, and this issue will be further elaborated on in a future DAVID report.

VII. E-MAIL ARCHIVING IN PRACTICE

A. INTRODUCTION

Each institution chooses the e-mail archiving strategy that best suits its organisation, computer infrastructure and e-mail policy. The options elaborated above can be applied in different ways and in several combinations. A variety of examples is available. New Zealand's *National Archives* prefer paper archiving of e-mails[75]. The Dutch province of Zeeland prints its e-mails on paper and does not digitally collect them[76]. The American GRS20 standard originally used the two options next to each other. E-mails with short-term archive value remain stored within the e-mail system. E-mails with long-term archive value are printed and added to the paper case. The current version of the GRS20 standard allows digital and hard copy (paper, microfiche) archiving[77]. The Canadian National Statistics Department has

[75] http://www.archives.govt.nz/statutory_regulatory/er_policy/chapter_5_frame.html

[76] J. JONKERS, *Zeeland gaat digitaal: studiedag over elektronisch documentmanagement*, in: *Od*, September 2001, nr. 9, p. 349

[77] http://www.nara.gov/records/grs20/

its staff send the e-mails with archival value to a central mailbox where they are classified, linked and archived by records managers. The Dutch Home Secretary will soon introduce a similar approach.

An example in the shape of a good practice will be elaborated on below. The goal is to compose an electronic archiving strategy that meets the predetermined quality demands. Electronic archiving is preferred to paper prints because e-mails are primarily electronic and because of the advantages connected to electronic archiving: automatic querying, sorting and indexing, central management, decentralised and simultaneous usage, etc.

The technological infrastructure is an important factor that has to be kept in mind when drawing an archiving strategy. The available computer infrastructure will largely determine what the archiving process will look like. Not every Flemish institution or department has the possibility to adapt its computer infrastructure to its archiving strategy. Because of this a solution has been found that can be applied to as many different widespread computer applications as possible.

The good practice consists of the archiving of e-mails as separate XML files in a folder structure outside the e-mail system and within the organisation's document management or recordkeeping system[78]. The recordkeeping process consists of a number of steps:

- STEP 1: The e-mails contain all transmission data and a reference to the context
- STEP 2: The e-mails with archival value are temporarily stored in a folder structure
- STEP 3: The e-mails are incorporated in the document management or recordkeeping system and grouped with all related documents.

B. GOOD PRACTICE

Step 1: The e-mails contain all transmission data and a reference to the context

In a first step it will be ensured that all e-mails explicitly contain all transmission data and a reference to their context and attachments. It has been mentioned before that this also needs to be verified when taking the hard copy option.

An organisation will archive both outgoing and incoming e-mail. Both types of e-mail should contain all transmission data and a reference to context and attachments. To achieve this it is best to adapt the e-mail templates. Most e-mail systems use the same default template for the e-mails in the folders 'Inbox' (incoming messages) and 'Sent Items'[79]. This template usually lacks the default mentioning of date and

[78] This best practice will become reality when the Antwerp City Archives will archive the e-mails of the Antwerp City administration.

[79] The common client e-mail programmes can automatically store a copy of each outgoing e-mail in the folder sent (items).

time of reception. For most common e-mail programmes all other transmission data (name sender, name addressee, receiver(s) of the copy/copies, subject, date and time of sending) usually does form part of the template for incoming e-mails. Many widespread e-mail client programmes such as MS Outlook and Lotus Notes allow the user to adapt the templates. Adding a field for date and time of reception to the e-mail header will assure that this information is explicit part of the archived e-mail. Sometimes it needs to be specified that this newly added field has to be printed or exported as well.

The standard templates often lack also the space to add a reference to the context and attachments of the e-mail message. That context relates to the work process in which the e-mails were created, received or used and to the other documents concerning the same case or subject. It is best to use a classification code or a case number to indicate the link with a certain work process. In ou solution, the template for outgoing mails contains a field where the sender can note his or her classification information[80]. In the example below this field is called 'FILE'. The content of this field refers to the case or the subject related to which the e-mail needs to be situated. A similar solution is applied for the reference to the attachments of the e-mail message. An additional field 'ATTACHMENTS' is added to the same template[81]. This is the way the e-mail message is linked to its attachments. During the recordkeeping process the messages are separated from the attachments; explicitly storing what attachments were sent together with the message ensures this relation is kept intact.

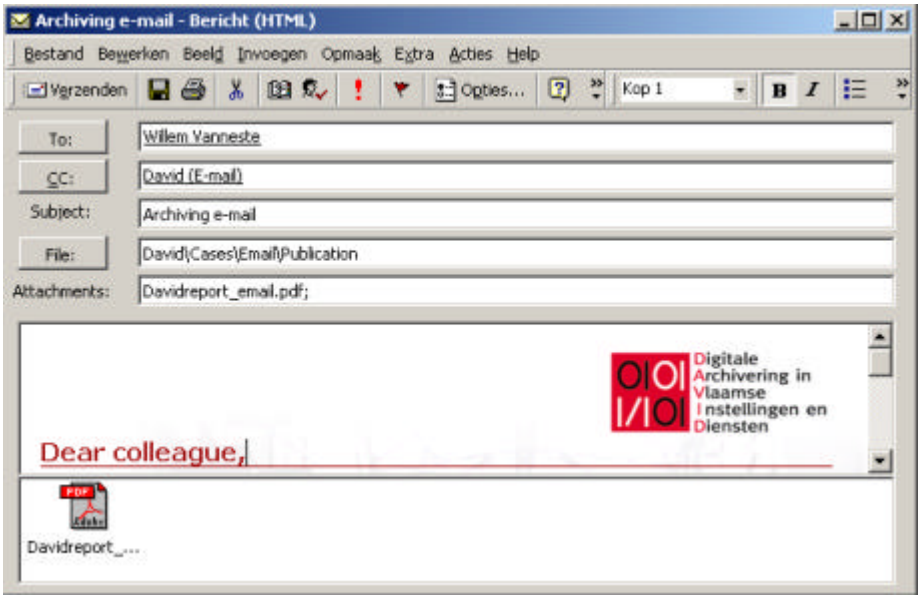


Image 7:
The adapted form for outgoing e-mail. The user can browse for the name of the file/subject or he fills this is in manually. The filenames of the attachments are automaticly registered in the field 'ATTACHMENTS'.

To facilitate the use of the extended e-mailheaders two scripts are added to the composepage of this form. The sender can always fill out the additional fields manually, but this isn't user-friendly and the

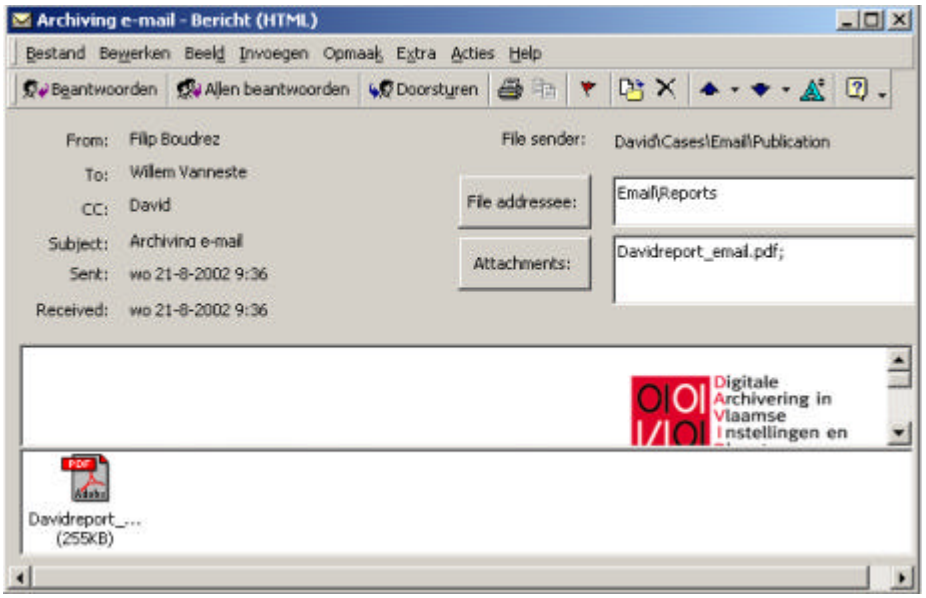
[80] It would also be possible to add the classification information in the field 'subject'. This would imply however that the addressees would receive e-mails with a subject that means nothing to them. And some space needs to be foreseen anyway for the classification information of the addressee.

[81] This is slightly different from the e-mailheaders in images 3 and 4. Because in the example of image 7 the field 'ATTACHMENT' is automaticly filled in, two different fields for data about the attachments are superfluous. In images 3 and 4 the first field will store the number of attachments; the second field will clarify what attachments these are (for example via a description or via file names).

chance exists that he "forgets" to fill them in. The button 'FILE' lets the sender browse for the corresponding filefolder and returns the path/foldername. A second script automaticly fills in the filenames of the attachments when the sender inserts them in the mail.

Adapting the template for outgoing e-mails is only necessary to allow the sender to explicitly add the necessary contextual information. His outgoing e-mails will end up in the template for incoming e-mails in the folder ‘Sent items’. This implies that also the template for incoming e-mails requires modification. The same work method is applied for this. Some extra fields are added to the e-mail header. A first extra piece of information is the date and time of reception. Also the fields ‘FILE SENDER’ and ‘ATTACHMENTS’ will be added to the header. The field ‘FILE SENDER’ is read-only. The field related to the attachments can be modified if necessary. It occurs all the time that an attachment with that file name already exists in the destination folder. The reference in this field has to change when the filename is adopted during the export. The button behind 'ATTACHMENTS' automaticly fills in all the filenames of the attachments. E-mails received from outside the own organisation can contain attachments but their senders won't have the adapted e-mailheaders. Finally this header is extended with a field where the addressee can fill in his own classification information: 'FILE ADDRESSEE'. Just like the sender, he can browse for the filename. This field will remain empty when the sender archives his outgoing e-mails.

Image 8:
To allow the archiving of incoming and outgoing e-mails including the necessary transmission and contextual information, the standard header for incoming e-mails has been extended with the following fields: reception date and time, classification information of the sender and the addressee, number of attachments and attached files.



The e-mail, as it reaches the folder ‘Sent items’, does not require adaptations for the archiving of outgoing e-mails. The sender has already added a reference to the context and possible attachments in the header when composing an outgoing messages. When archiving incoming e-mail the addressee needs to store the archival bond in the field ‘Classification addressee’ by means of some classification information. Then he or she can store the e-mail. The content of this field is now added to the incoming e-mail.

Adding a reference to the attachments and the context has the advantage that this essential information now becomes an inseparable part of the e-mail message. Transmission data will be automatically registered by incorporating it explicitly in the e-mail headers. This is an application of the encapsulation principle where the necessary metadata is incorporated in the electronic record itself. This information can then be perfectly managed within an existing e-mail system. The additional fields could be incorporated both in the header and in the body but preference lies with the e-mail header. This is not just adding some sort of metadata: adding this information to the header allows a clearly structured storage. Archived e-mails can then later be retrieved or sorted based on this information. The transmission and contextual data will later be transposed to XML as part of the e-mail message. This also guarantees a durable, platform independent and accessible storage of this essential metadata.

Step 2: The e-mails with archival value are stored in a folder structure

The e-mails with archival value will be moved from the folders 'Inbox' and 'Sent items' to the folder containing the e-mails related to the file or subject.

The sender and the receiver perform this action. This implies that a difference is being made between e-mails with and without archival value. This distinction should not be pushed aside when implementing an archiving strategy. Moving e-mails to folders implies appraisal and consequences for retrieval, disposition or preservation. The (administrative) assistants will perform a continuous selection and it must be clear which e-mails are to be stored and which are not. Some e-mails will be immediately deleted. These are in the first place the e-mails without record status. They can be personal e-mails or purely informative e-mails whose content is not related to the business process of the creator. In this phase the sender or the addressee should also reach an agreement about the storage of internally widespread e-mails. The sender should store e-mails that serve as general notifications within the proper organisation. The guidelines also discusses the so-called "reply mails". One has the choice here between archiving the last mail (that also contains all previous mails) or archiving each mail separately.

The e-mails with archival value are moved to the matching file or subject folder. All e-mails related to one subject or one case are thus grouped together. The folder structure is important as it integrates e-mails with the work process and the related documents. These related documents are not just the e-mail attachments but also all other paper or electronic documents that have been created within the organisation. One could choose to develop this folder structure within the e-mailsystem, on a shared (network)disk or a combination of both. Several scenario's are possible: store e-mails and attachments temporarily within the e-mailsystem and other internal electronic records on the shared disk, store only e-mails within the e-mailsystem and export attachments immediately to the folders with internal electronic records, immediately export e-mails and attachments to the folders on the shared disk where they are grouped into files with the internal documents, etc.

However, it must be clear that a folder structure within an e-mailsystem can only be a temporarily storage place for e-mails and possibly attachments. The folder structure within the e-mail system needs to match the classification of the paper records and/or the folder structure for electronic documents on the

shared network disks. After exporting them outside the e-mail system the e-mails will end up in the same folder structure. The connection between e-mails, attachments and other electronic documents related to the same case or subject will remain obvious by placing all computer files in the same folder.

The moment of exporting e-mails and/or attachments outside the e-mailsystem can be the moment when a case is closed, when a folder or mailbox has reached a certain size or when a certain period has expired. For reasons of sharing e-mails and attachments or filing all related documents, it can be appropriate to avoid temporarily storage within the e-mailsystem. In all cases, such an exporting moment should take place as close as possible to the time of sending or reception.

At the moment of filing outside the e-mailsystem, a decision will have to be made regarding to the target file format of the e-mail. One will have to choose between the native file format of the e-mailsoftware and the appropriate preservation format. Re-usability and future functionality are here important criteria. Choosing the native file format has the advantage that the e-mal easily can be opened in the e-mail clientsoftware, so responding or forwarding is still possible. This won't be that easy when the e-mail is stored in a acrhiving format such as XML or PDF for instance.

Storing e-mails in a folder structure is very similar to keeping a paper classification or efficiently managing shared work disks. The administration should have some experience with this. Yet it is advisable to give the necessary directions anyway. Coaching, guidelines and training for electronic recordkeeping must be more explicit than for the handling of paper records. The guideline should contain an answer to the following pratical questions: when is a public folder to be used and when an off-line folder? How should the folder structure be developed? How many levels are necessary in the structure? Who determines or changes the main structure? Some good examples can serve as a guide.

Step 3: The e-mails are incorporated in the document management or recordkeeping system

The archiving process should not stop after step 2. It is essential to incorporate e-mails in an document management or recordkeeping system because of accessibility, consultability, authenticity, reliability and further integration with the business process they support. A recordkeeping system is preferred, because it's better suited than a document management system to achieve this.

At the latest at this moment, the e-mails must be migrated to the appropriate archiving format. Several scenarios exist for the execution of the migration, but this process should be as automated as possible. Saving e-mails as XML-files is not a default functionality in the common e-mail systems, even in their most recent versions (MS Outlook 2002, Lotus Notes 5[82]). Considering the growing implementation of XML in software packages and the possible use of XML as messaging format[83] it is likely that future

[82] MS Outlook 2002 only contains the option to put individual e-mails in ASCII, RTF or Outlook file (*.msg) off-line. Lotus Notes can store e-mails as ASCII-, Lotus Ami Pro, Word, WordPerfect, TIFF and RTF file.

[83] G. KLYNE, *An XML format for mail and other messages*.

versions will have this functionality. For the moment, an ad hoc solution will need to be developed to enable the XML export from the current e-mail systems.

One possibility is a sort of plug-in that puts every e-mail outside the system as a separate Unicode file, tags that file and saves it as an XML file. A Visual Basic for Application macro in MS Outlook can perform this job for indivual e-mails or for the content of a whole Outlookfolder. Such a macro replaces a potential "save as…" function and operates fairly fast (faster than a PDF-writer/-distiller). Another possibility is a batch procedure that functions autonomously and that transposes off-line pst- or nsf files (*.pst, *.nsf). Both solutions require some programming work.

It is important that the archival bond remains intact during this operation. Archived e-mails need to stay in their folder and must contain all header information. When the transposition into XML takes place the e-mails are separated from their attachments. The technological link between e-mail and attachment will disappear after the transposition into XML. XML is the best archiving format for the e-mails themselves, but the attachments can be textual, graphical or audio-visual. Each type has a suitable file format for long term preservation. The attachments are no longer part of the e-mail but are separate files that are placed in the same folder as the e-mails and related electronic records. A de facto file will come into existence that collects all e-mails and attachments related to a given case or subject. Another option is to use XML as encapsulation format which contains besides the e-mail (header+body) also the textual encoding of the (binary) bitstreams of the attachment(s).

The last step is the ingestion of the archived e-mails in the organisation's document management or recordkeeping system. It is not enough to keep the e-mails in a folder structure on a hard disk of an external medium[84]. The archived e-mails should form part of the institution's global recordkeeping system that maintains the link and the context of the electronic records and that delivers the necessary functionalities. Amongs these, there is the protection of archived e-mails so changes or alterations aren' t possible. For the moment, the Antwerp City Records will take the archived e-mails into the document management system. A new object 'e-mail' has been designed with as attributes the metadata or header fields with context and transmission data. Bulk storage should be possible considering the amount of e-mails to be archived. Within the document management system the same folder structure will be applied. The preserved e-mails can be searched by browsing in the folder structure of by querying their metadata.

[84] The Australian National Archives Department for example considers this to be very important. The choice for electronic recordkeeping can only be justified if the archived e-mails are stored in a recordkeeping system. Without such a system the hard copy option is better-recommended (Archives advice, nr. 20).

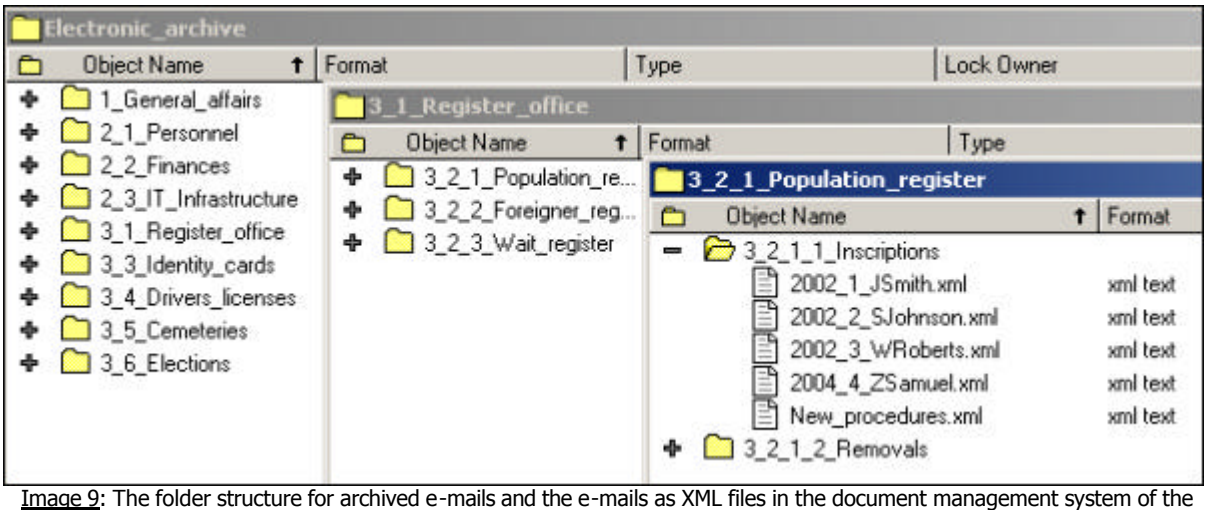


Image 9: The folder structure for archived e-mails and the e-mails as XML files in the document management system of the Antwerp City Archives. The folder structure is identical to the temporary folder structure in the e-mail system (see Image 2). The image has the main folders '3_1_Register_Office' opened in the e-mail archive. These folder consist of subfolders (tasks) that may again have been subdivided (activities).

C. Implementation in Practice

The good practice that has been presented here can be applied to different organisational structures and different technological infrastructures. It is irrelevant whether common e-mail addresses, personalised ones or a combination of both are used. The common e-mail systems allow the necessary functionality to allow or guide the creation of structured and contextualised e-mails. The main requirements towards the e-mail system are the possibility to adapt the headertemplates and to install a folder structure. The widespread e-mail packages also offer some query options.

Once the main action lines of the recordkeeping system have been determined, the implementation in practice can start. Implementing an e-mail recordkeeping system will be quite time consuming. The first two steps in this good practice can be executed rather quickly. It is even recommended to start them as early as possible. When the headertemplates have been adapted and the folder structure has been developed, the creation can start in a structured and contextualised manner. Meanwhile a way to implement the third step can be found.

A successful application will mainly depend on the administration. The Flemish administrations can't reckon on the services of records managers. This implies that the administration itself will be responsible for the application of the first steps in the archiving process: storing the context by efficiently filling in the header fields, selection, organisation and folder management. In other words, the administrative assistents will have to perform tasks that in other countries is entrusted to schooled and trained records managers. It goes without saying that these actions will require some training and coaching. It will not be enough to write only one memo with a general description of the procedure. The administration needs guidelines and examples, as concrete as possible. The City of Antwerp is organising courses on e-mail archiving and has a number of manuals and guidelines available on its intranet. One guideline describes the general archiving procedure; another contains advice and guidelines for an efficient folder structure. The e-mailusers are trained in dealing with the new e-mailheaders. The archivist will be the coach of this process and is co-responsible for the necessary training in appraisal and filing. Effective filing of the e-

mails in the corresponding folders is very important. Adding a certain e-mail to a folder has consequences for retrieval and will imply a decision regarding to disposition or preservation since appraisal and selection decisions will be made on folder level. One could compare this filing moment with the formel point when a document becomes a record.

Within most organisations the archivist will play the role of the architect of the recordkeeping system for e-mail archiving. Good co-operation with the computer responsible(s), more especially the network and e-mail server manager(s), will be essential.

The focal points of the archiving process explained above can also be used for retroactive incorporation of e-mails into the archive system. The San Diego Supercomputer Center has archived, as an experiment, one million e-mails in one day. The archiving consisted of tagging the messages, check-in into the recordkeeping system, indexing and description[85]. However retroactive contextualising is a different story. The e-mails sent or received before the coming into use of the adapted headers will have standard or adapted headers but will not contain a reference to the context. Contextualising would be possible by placing the e-mails in the matching folder and running a script which fills-in the reference to the context (foldername) into the e-mail header or body.

XIII. GENERAL CONCLUSION

This case clearly demonstrates the need to start the archiving process of electronic records as early as possible. From the moment of their creation actions are undertaken to allow efficient e-mail archiving. E-mailarchiving underlines the importance of the records continuumprinciple. Only starting the recordkeeping process when the transfer to the archive department takes place would threaten an archiving in a good, structured and accessible state. The selection and contextualising of the archived e-mails would be an impossible task.

The archiving of e-mails puts a big responsibility on the administration. It is responsible for the selection and the contextualising of the sent and received e-mails. It needs clear rules, as concrete as possible guidelines, and training. As the architect of the recordkeeping system the archivist is co-responsible for this.

The way in which e-mails will be archived shall differ from organisation to organisation. Printing e-mails is a valid option. This archiving method does not have technological difficulties and the archival bond to the context will be stored by the physical location of the print. The questions should be asked however for how long these option is sustainable and whether preserving prints is not a temporary solution during the transit from analogue to digital. It is important to assure that a printed e-mail contains all metadata.

[85] MOORE R., et.al**,** *Collection-Based Persistent Digital Archives - Part 2***.**

This can be easily realised by assuming all metadata as separate fields in the header of the e-mail forms or templates.

Electronic e-mail record keeping goes one step further by adapting the e-mail headers. As the context can only be stored in a logical or intellectual manner the header should foresee the necessary fields that indicate the link with the attachments and the context (case, subject). The e-mails can be temporarily stored within the e-mail system in an on-line or off-line folder structure. In a next phase the e-mails will be taken outside the e-mail system in a suited archiving format and next be incorporated into the document management or better a recordkeeping system.

Whichever option will be chosen, it is very important to respect the privacy regulations when archiving e-mail. Not the principle of confidentiality of mail but the principle of secrecy of telecommunication applies to the viewing and registration of (the content of) e-mails. Even though this regulation is not (yet) adapted to everyday practice, the archivist must keep it into account and must ensure that the registration of e-mail takes place according to the law as much as possible. When considering the importance of the employee's privacy and the importance of the organisation to possess a decent archive, it is always the principle of "a reasonable expectation of privacy" that should prevail. This expectation should be clearly communicated to those involved. The e-mail policy should discuss this matter in an unambiguous way.

BIBLIOGRAPHY

LEGISLATION AND REGULATIONS

BOOKS

DUMORTIER, J., *Informatica- en telecommunicatierecht*, Leuven, Acco, 2001, 226 p.

MAST, A. and DUJARDIN, J., *Overzicht van het Belgisch grondwettelijk recht*, Brussels, Story-Scientia, 1987, XXVII, 617 p.

HENDRICKX, F., *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, XXI, 358 p.

NOUWT, S., *Toepassing van privacyregels op elektronische berichten: Privacyregels voor internetberichten; Privacyregels voor EDI-berichten*, Deventer, Kluwer, 1999, 227 p.

VANDE LANOTTE, J., *Overzicht publiek recht*, Brugge, Die Keure, 2001, XLIX, 1291 p.

ARTICLES

DE HERT, P., 'Bedrijf mag post werknemers niet zomaar open maken', *Juristenkrant*, 2001, ed. 21, 5-6.

DE HERT, P., 'Schending van het (tele)communicatiegeheim in het beroepsleven', *T.S.R.*, 1995, 213-293.

DUMORTIER, J., 'Little Brother is watching you: mag de werkgever het Internetgebruik van zijn werknemers controleren?' in X., *Liber Amicoruum Prof. Dr. Roger Blanpain*, 1999, 243-259.

DUMORTIER, J., 'Internet op het werk: controlerechten van de werkgever', *Oriëntatie*, February 2000, 35-42.

KUITENBROUWER, F., 'Inzage e-mailberichten politie-ambtenaren door werkgever', noot onder Registratiekamer, brief d.d. 14 October 1997, feature 97\0578.1, *Computerrecht*, 1998, nr. 5, 253-254.

HORSMAN, P., Archivering van Elektronische Post. Methoden, meningen en alternatieven, Archiefschool Amsterdam, 1999, 9, available on http://www.archief.nl/digiduur/bibliotheek/archelp.pdf.

LEBOUTTE, J.M., 'De wettelijke bescherming van het briefgeheim', *De Gemeente*, 1988, 369-371.

SUYKENS, M., 'Briefgeheim bij openbare besturen', *De Gemeente*, 1995, nr. 4, 182-184.

VAN VAERENBERGH, E., 'Wettelijke bescherming van het briefgeheim', *De Gemeente*, 1989, 165-166.

WALLACE, D., Recordkeeping and Electronic Mail Policy: The State of Thought and the State of the Practice, paper prepared for the Annual Meeting of the Society of American Archivists, Orlando, Florida, September 3, 1998,
Available on http://www.rbarry.com/dwallace.html

ARCHIVISTIC PART

Archives advice 20. E-mail is a record!
Available on http://www.naa.gov.au/recordkeeping/rkpubs/advices/advice20.html

E-mail http://www.nla.gov.au/padi

E-mail policies in the government of Canada. A directory. Ottawa, 1996.

Guideline for Managing E-mail, Kansas, 2000.

Managing electronic messages as e-mails. Guidelines.
http://www.naa.gov.au/recordkeeping/er/elec_messages/contents.html

Managing electronic messages as e-mails. Policy.
Available on http://www.naa.gov.au/recordkeeping/er/elec_messages/contents.html

Managing electronic messages as records.
Available on http://www.gslis.utexas.edu/~scisco/lis389c.5/email/index.html

Managing e-mails as record. Website of the Managing Electronic Records Seminar, Technological summer camp at the University of Texas,

Available on http://www.gslis.utexas.edu/~scisco/lis389c.5/email

DURANTI, L., *The archival bond*, in: *Archives and museum informatics*, 1997, nrs. 3-4, p. 213-218.

JANSEN, D., *Archiving E-Mail & Public Records: Challenges, Strategies, & NARA's Electronic Records Archives*. Available on http://www.nara.gov

MOORE, R., et.al., *Collection-Based Persistent Digital Archives-Part 1*, in: D-LIB Magazine, March 2000. Available on http://www.dlib.org

MOORE, R., et.al, *Collection-Based Persistent Digital Archives - Part 2*, in: D-LIB Magazine, April 2000.

THIBODEAU, K., MOORE, R. and BARU, C., *Persistent Object Preservation: Advanced Computing Infrastructure for Digital Preservation*, in: *Proceedings* of the DLM Forum on electronic records. European citizens and electronic information: the memory of the Information Society, Brussels, 1999, p. 113-120.

THIBODEAU, K., *Preservation and Migration of Electronic Records: The State of the Issues,* available on http://www.nara.gov/era/kt_preservation_and_migration.html

THIBODEAU, K., *Building the Archives of the Future*, in: D-Lib Magazine, February 2001.

THOMASSEN, T.H.P.M., *Een korte introductie in de archivistiek*, in: P.J. HORSMAN, F.C.J. KETELAAR, THOMASSEN, T.H.P.M., *Naar een nieuwe paradigma in de archivistiek*, 's Gravenhage, 1999, p. 11-20.

ANNEX 1: E-MAIL POLICY

When implementing an electronic mail system within the government it is not just the latest technological developments that matter: there is also a need for clear procedures that take the different functions a government has to fulfil into account. The lack of a government e-mail policy or the existence of such a policy that does not take the e-mail storage issue into account could cause civil servants to consider e-mail as an informal means of communication and not as a possible record to be archived. This is the case for most of the Flemish governments. In this section we will examine what archiving aspects an e-mail policy should contain. These guidelines should help the Flemish administrations to compose their proper e-mail policy. The starting point will not be the introduction of a new set of barriers but the establishment of a careful government communication and information policy.

Composing an e-mail policy is often confided to the legal department of the organisation, however without a good reason. It is clear that lawyers should review the policy to make sure it complies with the relevant legal rules. However this review should only be the final step in the development of that e-mail policy[86]. A legal analysis should be considered as an addition to the policy as it has been developed for this particular organisation. In any case it is vital that archivists and record keepers co-operate. It is also important that they will later convincingly explain to their colleagues in the organisation why the policy has been composed in this particular way, as far as the policy itself does not demonstrate this. Rules are better followed up if it has been made clear why they exist.

The e-mail policy of any Flemish administration should take the following aspects of archiving into account:

1. <u>The status of 'record'</u>

An e-mail policy should not only determine that an e-mail can be a record of the administration, it should also clearly fix the conditions for it to be a functional e-mail. It should be clear when the organisation is to consider the e-mail as a record. These determinations will be more compelling and understandable for the end user when the policy not only defines records in terms of company activity and e-mail format, but also gives concrete examples that can be found within the organisation.

Furthermore it needs to be clearly stipulated which functional e-mails are formal and may therefore not be destroyed by the end user without the prior consent of the authorised persons within the organisation. Not every e-mail that is a record needs to be stored. It could be useful to refer to the stipulations or regulations that define the storage of specific records. This will make it clear to the end user why he or

[86] DUMORTIER, J., Regulating and monitoring communications in the enterprise: guidelines for the development of an effective usage policy, paper prepared for the On-line Rights Conference

she cannot delete certain e-mails. Public administrations can refer in their e-mail policy for example to the Archive Act and the Access Laws.

2. Access to e-mail facilities and personal usage

More and more guidelines about personal usage of the e-mail system appear in existing e-mail policies. They limit the usage of personal e-mail traffic or exclude it completely. These policies usually worry about the organisation's productivity and want to ban unproductive e-mail traffic from the organisation. Ensure that these guidelines also consider the archiving aspect, for example by stipulating that personal e-mail traffic needs to take place via a separate e-mail address. To respect the end user's freedom to communicate it is recommended to allow some private usage of the e-mail facilities but to make clear that all e-mail in the electronic mailbox will be considered to be functional e-mail.

An administration not only needs to determine who receives e-mail facilities under what conditions, it also needs to oblige those end users that possess e-mail facilities to check their electronic mailbox for incoming messages on a regular basis. This will assure treatment of correspondence within a reasonable term. The European Code of good administrative behaviour determines that for each letter the administration receives a receipt should be sent within two weeks.

3. The reasonable expectation of privacy

The previous part has demonstrated that there are two conflicting interests: the end user's right to privacy and the organisation's right (and often duty) to possess a well-structured and complete archive. The end user's privacy will need to be touched in any case. That is why it is important for the end user to realise what he can expect as far as privacy is concerned.

Clearly indicate whether the organisation reserves the right to check the content of the electronic mailbox for archiving purposes and if so (this will be the case for all large organisations) how the permission of those involved will be asked. Make clear that the organisation will consider all e-mails found in the electronic mailbox to be records belonging to the organisation (see below). This will reduce the risk of a possible violation of the right to privacy. It has become clear that judges attribute great importance to privacy clauses in e-mail policies.

Also indicate the end user's responsibility towards the privacy policy, for example by the obliged use of a fixed clause. Realise that in some cases the permission of all those involved in the communication cannot be obtained for example because they are unknown or because the sender contacts the organisation spontaneously and for the first time.

4. Registration of e-mails

The same principle applies to e-mails as to letters: incoming e-mails cannot be centrally opened and read. If a government administration wishes to be able to assume that all incoming mail is only related to the working of the administration, it should use general e-mail addresses of the type 'name_department@name_administration.be'[87]. These e-mails can be centrally opened and read, as they do not arrive in the electronic mailbox of an individual civil servant. It goes without saying that this method will drastically facilitate the registration of e-mails. It can be enforced within the framework of the Access Laws by mentioning the general e-mail address on the correspondence and also by sending formal e-mails from this e-mail address.

5. Sending formal e-mail

Now that the legal status of an e-mail message has been arranged in the current legal framework and one can determine what e-mail can be used for in a correct way, the e-mail policy needs to stipulate which formal messages can be sent electronically and which cannot. The legal department is best placed to determine this; they will have to make an analysis of all possible outgoing administrative documents.

6. Recordkeeping

This part determines how the administration will keep the e-mails. There are several options: printing the e-mails and adding the prints to the paper cases, forwarding the e-mails with archive value to a central e-mail address for registration and storage, keeping the e-mails in off-line files, etc. The guideline also determines what should happen to the e-mails within the e-mail system after they have been printed or forwarded to a central mailbox.

7. Sorting e-mails

The end user knows best what the content of the e-mails is, what e-mails are related or what e-mails must be added to the case. That is why it must be predetermined that the end user is responsible to keep his electronic mailbox in order. This can be done using folders that reflect a certain sorting method. Each staff member or each department will develop an individual folder structure. This can refer to a manual for the installation of a folder structure.

[87] For example burgerlijke_stand@leuven.be or stadskantoor.linkeroever@stad.antwerpen.be

8. How to treat attachments

The e-mail attachments can overload the e-mail system and are often spreading viruses. What types of attachments are permitted? What is the maximum size of sent attachments? Some companies do not allow the addressee to open the attachment without the computer responsible first scanning the attachment for viruses. The policy should also answer the question of how attachments with archive value are to be archived. Paper archiving allows the attachments to be printed and added to the case or subject folder. Digital archiving has the choice between temporary storage within the e-mail system and immediate storage outside the e-mail system.

9. Storage period

It will usually suffice to refer to the storage period of paper archive records.

10. How to treat encryption

The e-mail policy should mention the organisation's attitude towards encryption from an archivist point of view. Encryption can be used to add a digital signature to an e-mail. In this case the content of the e-mail will reach the addressee in a legible form. However it is also possible that the communication partners decide to encrypt the message itself to assure confidentiality of its content[88]. Here the legibility should be considered against the confidentiality of the e-mail traffic. Archivists will stress the legibility and will therefore have a negative attitude towards e-mail encryption. It should be pointed out that the law starts from a principle confidentiality of e-mail. All authorised measures can be taken to ensure this confidentiality during the transfer. And even if the right to privacy of one's electronic message traffic has been put aside towards one's employer, it goes still a bit too far to claim that the administration can forbid the encryption of e-mail. Furthermore this encryption can be to the benefit of the organisation for example when communicating confidential information.

11. Responsibility

The e-mail policy should determine a reference point that one can turn to when problems arise about the application of the policy. It is not necessary to have one single reference point for the whole policy. For problems related to the storage of e-mails the records manager seems to be the preferred reference point.

[88] This implies in practice that the sender will encrypt the message with the addressee's public key, so that only the addressee is capable of decrypting the message with his private key.

12. Sanctions

The sanctions that apply when the policy is not complied with should be clearly described. This gives the policy a more enforceable nature. The sanction can be to deny the person involved access to all information technology within the organisation. In Belgium however neither the Archive Act nor the Access Laws contain a sanction for persons destroying government documents including e-mails[89]. The Canadian *Freedom of Information and Protection of Privacy Act* stipulates that it is a crime to deliberately destroy documents, including e-mails and security copies, if the goal is to prevent an access request to these documents by a public institution.

[89] However Article 241 of the Criminal Code will punish all public officers or civil servants and all persons executing public services who deliberately or fraudulently delete or make disappear any documents or titles that are stored under their responsibility (meant are public notaries and registrars of mortgages but also archivists in public service). The punishment consists of five to ten years of prison and a fine of fifty to thousand francs (x two hundred).

ANNEX 2: DTD & XML SCHEME FOR E-MAIL

Strictly speaking the archiving of e-mails as XML files does not require a DTD or XML Scheme. To check the transposition into XML it is possible to build in a parsing.

A. DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT email (sender, sent, addressee, received, copie_to, context,
attachments, subject, message)>
      <!ELEMENT sender (name, address)>
            <!ELEMENT name (#PCDATA)>
            <!ELEMENT address (#PCDATA)>
      <!ELEMENT sent (#PCDATA)>
      <!ELEMENT addressee (name, address)>
      <!ELEMENT received (#PCDATA)>
      <!ELEMENT copie_to (name, address)>
      <!ELEMENT context (file_sender, file_addressee)>
            <!ELEMENT file_sender (#PCDATA)>
            <!ELEMENT file_addressee (#PCDATA)>
      <!ELEMENT attachments (#PCDATA)>
      <!ELEMENT subject (#PCDATA)>
      <!ELEMENT message (#PCDATA)>
```

B. XML SCHEME

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2000/10/XMLSchema"
elementFormDefault="qualified">
      <xsd:element name="name" type="xsd:string"/>
      <xsd:element name="address" type="xsd:string"/>
      <xsd:element name="sent" type="xsd:date"/>
      <xsd:element name="received" type="xsd:date"/>
      <xsd:element name="subject" type="xsd:string"/>
      <xsd:element name="file_sender" type="xsd:string"/>
      <xsd:element name="file_addressee" type="xsd:string"/>
      <xsd:element name="attachments" type="xsd:string"/>
      <xsd:element name="message" type="xsd:string"/>

      <xsd:element name="sender">
      <xsd:complexType>
            <xsd:sequence>
                  <xsd:element ref="name"/>
                  <xsd:element ref="address"/>
            </xsd:sequence>
      </xsd:complexType>
      </xsd:element>
```

```
      <xsd:element name="addressee">
      <xsd:complexType>
            <xsd:sequence>
                  <xsd:element ref="name"/>
                  <xsd:element ref="address"/>
            </xsd:sequence>
      </xsd:complexType>
      </xsd:element>

      <xsd:element name="copie_to">
      <xsd:complexType>
            <xsd:sequence>
                  <xsd:element ref="name"/>
                  <xsd:element ref="address"/>
            </xsd:sequence>
      </xsd:complexType>
      </xsd:element>

      <xsd:element name="context">
      <xsd:complexType>
            <xsd:sequence>
                  <xsd:element ref="file_sender"/>
                  <xsd:element ref="file_addressee"/>
            </xsd:sequence>
      </xsd:complexType>
      </xsd:element>

      <xsd:element name="email">
      <xsd:complexType>
            <xsd:sequence>
                  <xsd:element ref="sender"/>
                  <xsd:element ref="sent"/>
                  <xsd:element ref="addressee"/>
                  <xsd:element ref="received" minOccurs="0"/>
                  <xsd:element ref="copie_to" minOccurs="0"/>
                  <xsd:element ref="subject" minOccurs="0"/>
                  <xsd:element ref="context" minOccurs="0"/>
                  <xsd:element ref="attachments" minOccurs="0"/>
                  <xsd:element ref="message" minOccurs="0"/>
            </xsd:sequence>
      </xsd:complexType>
      </xsd:element>
</xsd:schema>
```