Digital archiving: the new challenge?

F. Boudrez, H. Dekeyser and Prof. J. Dumortier

legal and archival issues

Filip Boudrez (Stadsarchief Antwerpen)
Hannelore Dekeyser and Prof. Jos Dumortier (ICRI – K.U.Leuven)

Image Recognition
Integrated Systems Group S.A.
Professional Solutions
Rue du Bosquet 10
Parc Scientifique de Louvain-la-Neuve
1435 Mont Saint Guibert
Belgium
tel. +32 10 48 75 30
fax +32 10 48 75 40
www.irislink.com

Digital archiving: the new challenge?
Digital archiving: the new challenge? 

Legal and archival issues
TABLE OF CONTENTS

PREFACE 7

Part 1: The Legal Framework for Business Archives

A. WHY DO WE PRESERVE DOCUMENTS? 13
B. THE ORGANIZATION OF THE ARCHIVE 14
C. DIGITAL DOCUMENTS: DEFINITION OF THE PROBLEM 15
D. GENERAL FRAMEWORK: THE LAW OF EVIDENCE 16
E. THE ELECTRONIC COMMERCE ACT 24
F. BOOKKEEPING AND ANNUAL ACCOUNTS 27
G. SOCIAL DOCUMENTS 34
H. MEDICAL FILES 39
I. PRIVACY 43
J. COPYRIGHT AND NEIGHBORING RIGHTS 49

L. ANNEX 1. THE DIGITAL SIGNATURE TECHNOLOGY 68
K. CONCLUSION 69

Part 2: Electronic Record Keeping

A. INTRODUCTION 75
B. PRESERVATION STRATEGIES 81
C. ARCHIVING STANDARDS 89
D. POLICY AND PROCEDURES 96
E. ARCHIVING PROCEDURES 102
F. CONCLUSION 125

REFERENCES PART 1 127
REFERENCES PART 2 133
How a business problem in combination with increasing strict legislation can motivate organizations to develop successful strategies and competitive advantages.
Regardless of the economic situation, we are faced with an exponential increase in the amount of information circulating within our organizations. Though only a fraction can truly be used for business, we are condemned to develop strategies to archive and store this data. Electronic archiving has become crucial and entails the identification of appropriate solutions to related technical problems. Therefore, while in the past organizations were forced by necessity to electronically archive data useful for their business, they now must also satisfy increasingly broad requirements to follow precise electronic archiving rules. IT departments are no longer the only entities to suffer from this problem. Organizations as a whole in all business departments are concerned. Knowledge is the most important asset. It must, therefore, be protected, managed, preserved, circulated, exchanged and made safe. For these reasons, archiving is one of the key issues facing organizations.

More than 10,000 laws and norms form the legal framework regulating archiving in the US. Though the system is not yet as complex in Europe, norms developed in the US have rapidly leaked throughout the world, through subsidiaries of American companies, for example. In addition, discussions to this effect have already taken place at the European Communities level and within most European countries. Various texts regulate proof of electronic signature, preservation of electronic documents or even electronic billing. Specific regulations have been implemented in certain sectors such as social security, retirement funds, income tax or VAT declarations, etc. The ISO and AFNOR (French Association of Normalization) have published legal archiving procedures and regulations.

The Sarbanes-Oxley Act adopted in July 2002 creates a stringent set of rules for reporting financial information. Companies must provide access to their accounts and the CEO and CFO must personally certify the authenticity and reliability of financial information. Increased responsibility of company executives and independence of auditors have been enforced. The law was adopted to restore investor confidence lost as a result of various scandals such as those concerning Enron, WorldCom and others. This law is followed by these overall principles concerning electronic work. In addition, discussions have already taken place at the US Securities and Exchange Commission (SEC) level and within most US securities exchanges about the introduction of controls over every aspect of electronic archiving. The problem of compliance is at the heart of this issue. The regulations were designed to define the way in which companies create, store, consult, preserve and archive recorded data (information in various forms) for increasing durations of time. If companies do not comply with these archiving system requirements, heavy fines could be imposed on them.

The Sarbanes-Oxley Act, adopted in July 2002, creates a stringent set of rules aimed at restoring investor confidence lost as a result of various scandals such as those concerning Enron, WorldCom and others. This law is guided by these overall principles concerning electronic work. In addition, discussions have already taken place at the US Securities and Exchange Commission (SEC) level and within most US securities exchanges about the introduction of controls over every aspect of electronic archiving. The law was adopted to restore investor confidence lost as a result of various scandals such as those concerning Enron, WorldCom and others. This law is followed by these overall principles concerning electronic work. In addition, discussions have already taken place at the US Securities and Exchange Commission (SEC) level and within most US securities exchanges about the introduction of controls over every aspect of electronic archiving. The problem of compliance is at the heart of this issue. The regulations were designed to define the way in which companies create, store, consult, preserve and archive recorded data (information in various forms) for increasing durations of time. If companies do not comply with these archiving system requirements, heavy fines could be imposed on them.

The Sarbanes-Oxley Act, adopted in July 2002, creates a stringent set of rules aimed at restoring investor confidence lost as a result of various scandals such as those concerning Enron, WorldCom and others. This law is guided by these overall principles concerning electronic work. In addition, discussions have already taken place at the US Securities and Exchange Commission (SEC) level and within most US securities exchanges about the introduction of controls over every aspect of electronic archiving. The problem of compliance is at the heart of this issue. The regulations were designed to define the way in which companies create, store, consult, preserve and archive recorded data (information in various forms) for increasing durations of time. If companies do not comply with these archiving system requirements, heavy fines could be imposed on them.

The Sarbanes-Oxley Act, adopted in July 2002, creates a stringent set of rules aimed at restoring investor confidence lost as a result of various scandals such as those concerning Enron, WorldCom and others. This law is guided by these overall principles concerning electronic work. In addition, discussions have already taken place at the US Securities and Exchange Commission (SEC) level and within most US securities exchanges about the introduction of controls over every aspect of electronic archiving. The problem of compliance is at the heart of this issue. The regulations were designed to define the way in which companies create, store, consult, preserve and archive recorded data (information in various forms) for increasing durations of time. If companies do not comply with these archiving system requirements, heavy fines could be imposed on them.

The Sarbanes-Oxley Act, adopted in July 2002, creates a stringent set of rules aimed at restoring investor confidence lost as a result of various scandals such as those concerning Enron, WorldCom and others. This law is guided by these overall principles concerning electronic work. In addition, discussions have already taken place at the US Securities and Exchange Commission (SEC) level and within most US securities exchanges about the introduction of controls over every aspect of electronic archiving. The problem of compliance is at the heart of this issue. The regulations were designed to define the way in which companies create, store, consult, preserve and archive recorded data (information in various forms) for increasing durations of time. If companies do not comply with these archiving system requirements, heavy fines could be imposed on them.

The Sarbanes-Oxley Act, adopted in July 2002, creates a stringent set of rules aimed at restoring investor confidence lost as a result of various scandals such as those concerning Enron, WorldCom and others. This law is guided by these overall principles concerning electronic work. In addition, discussions have already taken place at the US Securities and Exchange Commission (SEC) level and within most US securities exchanges about the introduction of controls over every aspect of electronic archiving. The problem of compliance is at the heart of this issue. The regulations were designed to define the way in which companies create, store, consult, preserve and archive recorded data (information in various forms) for increasing durations of time. If companies do not comply with these archiving system requirements, heavy fines could be imposed on them.
The Sarbanes-Oxley Act is applicable to companies, banks and savings associations that file reports with the SEC under section 13(a) or 15(d) of the Securities Exchange Act of 1934. Thus, this concerns all listed companies. The transitory measures will expire the 15th of April 2005 and, thus, the Sarbanes-Oxley Act will come into full effect without exception. On one hand, all non-American companies with activities in the US and that file reports with the SEC must comply with the act for all their activities. On the other, all subsidiaries and branches of American companies throughout the world that file reports with the SEC must also comply. Therefore, to a certain extent, this law is universal.

The Sarbanes-Oxley Act does not define the conditions for appropriate internal control, but the SEC did create an internal control structure (Committee of Sponsoring Organizations or COSO) that meets its criteria for evaluation and development of controls. COSO defined five components of effective internal control: control environment, risk assessment, control activities, information and communication and, lastly, monitoring. Since the 26th of April 2003, companies work with independent verification committees to monitor the verification process. These independent committees are authorized to receive complaints from shareholders or employees concerning the company's accounting procedures and verification procedures.

Concerning the control environment, the COSO stresses the importance of the assignment of authority and responsibility: the management of identities and access is crucial. In the area of control activities, the COSO requires company management to define the policies, procedures and specific actions necessary to manage the risks associated with the specific controls. Management must evaluate the design and operational efficiency of these specific controls to deal with the risks they intend to address.

The COSO also defined the control measures specifically applicable to IT. Several companies based their measures on COBIT (Control Objectives for Information and related Technology) published by the IT Governance Institute. These guidelines describe in detail the activities required for the evaluation of IT controls in order to comply with the Sarbanes-Oxley Act. The COBIT controls can be classified into four categories: planning and organization, acquisition and implementation, supply and support, and ongoing monitoring. Companies must develop procedures and verification procedures concerning the control measures that they believe are necessary to ensure that the controls are operating effectively.

The Sarbanes-Oxley Act also requires companies to report information to shareholders and employees concerning the effectiveness of their internal controls. Companies must disclose any material weaknesses in their internal controls or any changes in controls that are required to meet the Sarbanes-Oxley Act's requirements. Companies must also report any instances of fraud or misconduct by employees or others who have access to the company's financial records.

In summary, the Sarbanes-Oxley Act is a comprehensive law that sets high standards for corporate governance, financial reporting and internal controls. It has had a significant impact on the way companies operate and is widely regarded as a turning point in corporate accountability and transparency.
The Sarbanes-Oxley Act thus affects information systems on two levels:
– use of computers for management and financial control: each actor must be able to save data (bottom-up input) and management must be able to perform completely transparent controls (top-down visibility),
– requirement to certify computer system safety.

The opportunity to create a competitive advantage
It will certainly be a challenge for companies to comply with the requirements of the Sarbanes-Oxley Act and other current regulations.

However, several existing tools could serve as aids in this process:

- intelligent, indexed electronic documents allowing "full text" or fuzzy searches,
- scanning of incoming paper mail, indexation and integration into an electronic document management system,
- text recognition (OCR) from archived documents in image form to allow electronic document and workflow management so that the stage of the processing or handling of each scanned mail and work file’s text or data can be identified at any time,
- electronic document and workflow management of billing or automatic recognition of paper bills,
- archiving of e-mails, scanned mail and work files according to stringent procedures using reliable systems whose configuration meets standards defined by authorities,
- effective, highly regular backups.

The goal of this book is not to describe all the individual existing applications, but the role of archiving in the larger context of computer architecture and, more generally, of business needs.

The opportunity to create a competitive advantage
It is important to describe the role of archiving in the larger context of computer architecture and more generally of business needs. Several of these applications improve speed and accessibility, among other things:

- effective, highly regular backups,
- electronic document and workflow management so that the stage of the processing or handling of each scanned mail and work file’s text or data can be identified at any time,
- electronic document and workflow management of billing or automatic recognition of paper bills,
- archiving of e-mails, scanned mail and work files according to stringent procedures using reliable systems whose configuration meets standards defined by authorities,
- effective, highly regular backups.

It is important to describe the role of archiving in the larger context of computer architecture and more generally of business needs.

Several of these applications improve speed and accessibility, among other things.

The opportunity to create a competitive advantage
It is important to describe the role of archiving in the larger context of computer architecture and more generally of business needs.

Several of these applications improve speed and accessibility, among other things.

The opportunity to create a competitive advantage
It is important to describe the role of archiving in the larger context of computer architecture and more generally of business needs.
Like in many scenarios where reality evolves faster than fiction, laws have been slow to keep up with the breakneck speed of evolution of these technologies. The team led by Professor Dumortier in the Interdisciplinary Centre for Law and Information Technology (ICRI) has collaborated in the creation of several legislative initiatives at the European level. Their work has given us a view of the current situation in the area of computer law regulating archiving issues.

The DAVID system developed by the Archives of the City of Antwerp (Stadsarchief Antwerpen) is certainly one of the most successful electronic archiving systems. Its implementation by the team of Mr. Boudrez provided us with extremely enriching practical feedback.

Through the publication of this work, we hope to help heighten awareness about the fact that as technical solutions continue to evolve, the legal framework is adapted to allow organizations to define the guiding principles of policy for safety and competitiveness.

What is truly possible? What are the legal constraints? How does a complex archiving system really work? What are the pitfalls and opportunities?

We'd like to thank the BeLAIIM (Belgian and Luxembourgian Association for Information and Image Management) for their support of this initiative and their contribution to its success.

Happy reading!

Etienne Van de Kerckhove
CEO IRIS Group
Preservation is "the practical task that consists of keeping documents intact for future use." In preserving documents, we want to make and keep the information they contain available for the future. There are many different reasons for preserving documents. In the business community, documents are mainly preserved for legal reasons. Documents are kept because we are required to do so by law or because we are entitled to do so by virtue of a contract or for the sake of the evidence they provide. Legal reasons are important reasons for preserving documents. In the business community, documents are many preserved for legal reasons. Preservation is the practical task that consists of keeping documents intact for future use. There are two additional reasons for preserving documents. For society in general, historical and scientific research are two additional reasons for preserving documents. The preservation period as required by the law of evidence is determined by the statute of limitations established by civil law. The statute of limitations does not directly oblige anyone to preserve documents. However, as a consequence of the statute of limitations, the period within which a right can be enforced in court is limited. Anyone who destroys his evidence prematurely will have to bear the consequences when he can no longer demonstrate his rights before the court.

1. EVIDENCE LAW

A. WHY DO WE PRESERVE DOCUMENTS?

One of the paramount reasons for preserving documents is self-interest. The law grants many rights to natural and legal persons, but as a rule, one must be able to present evidence to prove that the conditions for obtaining these rights have been met. No one can predict whether and when a dispute will arise about the legal rights that he claims to have. Therefore it is important to preserve all documents that could support these claims. Furthermore, evidence must be preserved. Anyone who destroys evidence of his rights will find it difficult to prove that the conditions for obtaining these rights have been met. If someone wants to assert his rights on the basis of an agreement, he must first demonstrate the existence and validity of the agreement. If someone wants to hold another person liable for an error, he must first demonstrate the existence of an error, the harm suffered, and the causal relation between the two.

The preservation period as required by the law of evidence is determined by the statute of limitations. If the conditions for obtaining these rights have been met, the preservation period begins. If the conditions are not met, the preservation period does not start. The preservation period ends when the rights are no longer enforceable. Therefore it is important to preserve documents as long as the conditions for obtaining these rights are met. The preservation period is thirty years.
when the documents retain their authenticity, it must be possible to evaluate the
proceedings to reach the objectives desired above. Archiving only makes sense in all these cases. the term is extended under

Chapter 2: The Legal Framework for Business Archives

B. THE ORGANIZATION OF THE ARCHIVE

The public records act imposes a general obligation on the public sector to keep their records. There is no equivalent general obligation for the private sector. However, businesses must keep all the documents needed to determine their taxable income, whether declared income agrees with true income. Authorities have the power to examine the accounting books to determine whether declared income agrees with true income. Employers must keep all the documents needed to determine their taxable income, whether declared income agrees with true income. The tax authorities have the power to examine the accounting books to determine whether declared income agrees with true income. The rules on accounting are mainly intended to safeguard the rights of third parties. The public records act imposes a general obligation on the public sector to keep their records.

2. LEGAL OBLIGATION TO PRESERVE DOCUMENTS

For instance, when one of the parties is a minor, or by certain acts, such as the issue of a formal or an order of legal proceedings, for instance, to terminate the company. This chapter will give an overview of the law of evidence. The law of evidence contains the fundamental rules according to which all documents are judged in all areas of the law. The law of evidence contains the fundamental rules according to which all documents are judged in all areas of the law. The law of evidence contains the fundamental rules according to which all documents are judged in all areas of the law.
C. DIGITAL DOCUMENTS: DEFINITION OF THE PROBLEM

Authenticity and reliability of documents are often required when they are requested from the archive for reuse. A document is authentic if it is in reality what it purports to be. The authenticity of a document can be determined on the basis of its integrity and identity. All the information that is needed to determine the authenticity must be preserved in the metadata accompanying the document in the archive. Metadata include the author(s) and/or the person responsible for the document, the date, the (business) process within which it was created or received, etc. Archiving is first and foremost a practical task: in order to preserve a record, the appropriate technical and organizational measures must be taken.

Privacy regulations and copyright have a special impact on all aspects of archiving. The right to privacy limits the data that may be included in the archive. Any personal information in the archive must be stored carefully and may not be handed over to third parties. The inclusion in the archive of works protected by copyright requires, in principle, the permission of the copyright holders, as does modification and further distribution of the work.

Defining electronic document management with electronic storage of archival documents...
Part 1: The Legal Framework for Business Archives

Quickly and cheaply without too many formalities uses internet technology to keep in contact with customers and/or suppliers. Computer applications are widely used to steer and support internal operational processes. All this has led to a dematerialization of information transfer.

Today, many digital documents are still printed and then filed in paper form. This has led to a dematerialization of information transfer. Sophisticated electronic documents, such as databases and multimedia objects, cannot be printed to paper in a meaningful way. The deployment of electronic document management and archiving systems is the way forward.

However, several legal obstacles can stand in the way of the conclusion of contracts online. Prior to the implementation of such a system, the limits posed by law on the use of electronic documents must be researched and documented management systems must be implemented. However, several legal obstacles can stand in the way of the optimal use of such a system.

Evidence can be defined as demonstrating the accuracy of a fact or of the legality of an act. The Civil Code establishes a hierarchy of the various types of evidence because the law does not explicitly provide otherwise. The civil evidence rules apply in all areas of law, whereas, a contract or another legal act, the civil evidence rules apply in all areas of law.

Evidence can be defined as demonstrating the accuracy of a fact or of the legality of an act. The law of evidence is a determining factor for the way in which we archive documents. In addition, other legal rules that could impede the creation and/or preservation of legally relevant, electronic information should be taken into account. These sectoral rules often deviate from the law of evidence with respect to the method and terms of preservation. However, these sectoral rules often only concern the relationship between the taxpayer, the doctor or the employer with the government. With respect to others, it is evidence law that provides guidance for the preservation of documents and the evaluation of their legal value.

Evidence can be defined as demonstrating the accuracy of a fact or of the legality of an act. The Civil Code establishes a hierarchy of the various types of evidence because the law does not explicitly provide otherwise. The law of evidence is a determining factor for the way in which we archive documents.

Evidence can be defined as demonstrating the accuracy of a fact or of the legality of an act. The law of evidence is a determining factor for the way in which we archive documents.
2. A DOCUMENT SIGNED BY HAND

A document signed by hand is one that has been written or printed in a way that is legible and contains the signature of the person who has signed it. The signature is often placed on the document in a particular place or on a particular page. The signature is considered to be a form of evidence that can be used to prove the authenticity of the document.

The signature is often placed on the document in a specific location, such as the lower right corner of the document. The signature is usually written in ink or other permanent ink, and it is often initialed or dated.

The signature is considered to be a form of evidence that can be used to prove the authenticity of the document. In many jurisdictions, a signature is considered to be evidence of the person's agreement with the contents of the document. This is because the signature is considered to be a form of evidence that can be used to prove the authenticity of the document.

The signature is often placed on the document in a specific location, such as the lower right corner of the document. The signature is usually written in ink or other permanent ink, and it is often initialed or dated.

The signature is considered to be a form of evidence that can be used to prove the authenticity of the document. In many jurisdictions, a signature is considered to be evidence of the person's agreement with the contents of the document. This is because the signature is considered to be a form of evidence that can be used to prove the authenticity of the document.
1.8. The legal framework for business archives

A document is considered a copy when the signature appears in another form, for instance by using scanning techniques or microfilm. The law of evidence attributes greater value to an original document than to a copy. Article 1334 of the Belgian Civil Code stipulates that a copy will only be accepted as evidence when the original can still be produced. The opposing party can thus always challenge a copy and demand the submission of the original. This is very important when documentary evidence on paper is included in a digital archive (e.g. via scanning techniques). Usually the original is destroyed and can no longer be submitted. The electronic version is a copy because it lacks a valid signature and thus has only limited evidential value.

2. The electronic signature

In the past, the rules governing documentary evidence impeded the proof of agreements entered into electronically. The enforceability of these contracts in court was subject to great legal uncertainty as such agreements could not be signed by hand. Printing contracts concluded electronically could not provide a satisfactory solution. After all, the printout is a document that lacks an original signature and thus can at best be considered only a copy.

3. The electronic signatures act and certification service

Since 1 January 2001, new rules on the admission of electronic signatures have gone some way toward alleviating these problems. A digital document can now in principle fulfill the requirements of a signed document as the electronic signature is equivalent to a manual signature in the eyes of the law.

3.1. The electronic signatures act and certification service provider act

At the end of the 1990s, various European member states started adapting their rules of evidence to modern technologies. There was a fear that differing rules for the legal recognition of electronic signatures would arise within the European internal market. This could present serious obstacles for the development of electronic trade. That is why a directive was issued to create a common framework for electronic signatures. The directive was issued to create a common framework for electronic signatures. The enforceability of these contracts in court was subject to great legal uncertainty as such agreements could not be signed by hand. Printing contracts concluded electronically could not provide a satisfactory solution. After all, the printout is a document that lacks an original signature and thus can at best be considered only a copy.

The law of evidence considers a document on which the signature appears in another form (e.g. by using scanning techniques or microfilm) to be a copy and not an original. The opposing party can thus always challenge a copy and demand the submission of the original. This is very important when documentary evidence on paper is included in a digital archive (e.g. via scanning techniques). Usually the original is destroyed and can no longer be submitted. The electronic version is a copy because it lacks a valid signature and thus has only limited evidential value.
word processing file that contains the document he wishes to sign. The bitmap is created by scanning the signature. The users of this system use a password to gain access to their signature. Each of these three techniques captures the look and feel of a handwritten signature and this type of electronic signature will thus be easily recognized as a signature by layman. There are many other techniques besides this for creating an electronic signature. At present, the "digital signature" technique is the most advanced technique. In contrast to the digitized handwritten signature, the digital signature does not resemble the handwritten signature at all.

Since 1 January 2001, an electronic signature can also be considered as a valid signature subject to two conditions:

- It must be possible to attribute the electronic data that constitute the signature to a particular person (the signature’s identification and appropriation function)
- It must be possible to determine that the electronic data that constitute the signature have not been changed or destroyed in any way (integrity verification)

When the electronic signature satisfies these two conditions, it can be used as a valid signature by the judge. If he ascertains that one or both conditions are not satisfied, he will not accept the digital document submitted to him as a signed document, but as a normal document that he can evaluate for its credibility.

In the European context, considerable differences in interpretation could arise between member states with regard to which signature techniques are acceptable. To correct this, the directive has defined one type of electronic signature that must be accepted everywhere in the European Union as the equivalent of the handwritten signature. This type of signature is called a "qualified electronic signature." A description of a qualified electronic signature can be found in the Certification Services Provider Act. It is an "advanced electronic signature" based on a qualified certificate and created by a secure signature creation device. Each of these three techniques captures the look and feel of a handwritten signature and this type of electronic signature will thus be easily recognized as a signature by layman.

3.2. QUALIFIED ELECTRONIC SIGNATURES

A qualified electronic signature is a signature that is created and stored in electronic form. It is an "advanced electronic signature" based on a qualified certificate and created by a secure signature creation device. Each of these three techniques captures the look and feel of a handwritten signature and this type of electronic signature will thus be easily recognized as a signature by layman.

A qualified signature is first and foremost based on a technology that produces advanced electronic signatures. A qualified signature is created by a secure signature creation device. Each of these three techniques captures the look and feel of a handwritten signature and this type of electronic signature will thus be easily recognized as a signature by layman.

The contracting parties are entitled to choose from numerous techniques to sign their documents. The court may not ignore documentary evidence that is signed with an electronic signature solely because the signature is placed in electronic form. From now on, a digital document will only be considered as a signed document if the court is satisfied that the two conditions stated above are met.

These conditions are satisfied as follows:

1. The electronic data that constitute the signature must demonstrate the preservation of the document’s integrity.
2. The electronic data that constitute the signature must be attributed to a particular person.

In order to particularize the signature’s identification and appropriation function, it is necessary to attribute the electronic data that constitute the signature to a person. This person must be able to prove that he is the signatory by producing documentary evidence that he is the person who created the electronic signature.

In the digital environment, the signature does not resemble the handwritten signature at all. It is similar to a code of numbers that can be read by the computer but not by the human eye. The digital signatory’s name is written on the electronic document in the form of a code. This code must be used to sign the document.

This technique was first developed in the Netherlands. It is called the "qualified electronic signature." A description of a qualified electronic signature can be found in the Certification Services Provider Act. It is an "advanced electronic signature" based on a qualified certificate and created by a secure signature creation device. Each of these three techniques captures the look and feel of a handwritten signature and this type of electronic signature will thus be easily recognized as a signature by layman.

The court may not ignore documentary evidence that is signed with an electronic signature solely because the signature is placed in electronic form. From now on, a digital document will only be considered as a signed document if the court is satisfied that the two conditions stated above are met.

The qualified signature is first and foremost based on a technology that produces advanced electronic signatures. It is an "advanced electronic signature" based on a qualified certificate and created by a secure signature creation device. Each of these three techniques captures the look and feel of a handwritten signature and this type of electronic signature will thus be easily recognized as a signature by layman. A description of a qualified electronic signature can be found in the Certification Services Provider Act. It is an "advanced electronic signature" based on a qualified certificate and created by a secure signature creation device. Each of these three techniques captures the look and feel of a handwritten signature and this type of electronic signature will thus be easily recognized as a signature by layman.
Next, a qualified signature is accompanied by a qualified certificate. A certificate is qualified when it contains a certain set of information:

- the label "qualified certificate"
- contact information of the certification authority (CA)
- the certificate holder's name or pseudonym
- the period of validity
- signature verification data corresponding to the signature creation data held by the certificate holder
- the certificate's identity code
- the advanced electronic signature of the issuer of the certificate.

Where appropriate, the following information can be added:

- reference to a specific attribute of the signatory, for instance his profession
- the restrictions on the use of the certificate
- the limits relating to the value of the transactions for which the certificate may be used.

Certification authorities that wish to provide such qualified certificates must satisfy several conditions:

- they must demonstrate that they are sufficiently reliable to supply certification services;
- they must use trustworthy systems and protocols which are protected against modification and which guarantee the technical and cryptographic security of the processes that they support;
- they must employ personnel with the specific knowledge, experience and qualifications necessary to provide the services and in particular, to manage and maintain the processes and ensure proper security procedures and audit trails;
- they must be established in a Member State, in the current legal framework of which the certificate is issued and in an immediate revocation service;
- they must ensure the operation of a prompt and secure directory service;
- they must ensure that they are sufficiently reliable to supply certification services;
- they must be in a position to provide such qualified certificates;
- they must demonstrate that they are sufficiently reliable to supply such qualified certificates;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
- the limitations on the use of the certificate for which the certificate is intended;
they must notify every applicant for a certificate via a durable means of communication about the exact modalities and conditions for using the certificates, including the imposed limitations for their use, about the existence of a voluntary accreditation system and about the procedures for complaints and the settlement of disputes. This information, which can be transmitted electronically, must be in writing and formulated in language that is easy to understand. Upon request, relevant elements of this information must also be made available to third parties who rely on the certificate;

- they must use trustworthy systems to store the certificate in verifiable form so that:
  a) only authorized persons can enter and modify data;
  b) the authenticity of the information can be verified;
  c) the certificates will only become publicly available in the cases in which the certificate holder has granted his permission and
  d) the user must clearly understand each technical modification that poses a risk to security requirements.

Most of these conditions are rather vaguely formulated so it remains to be seen how they will be interpreted in practice. Certification authorities can request accreditation voluntarily from the Federal Public Service for Economy, SME’s, Self-Employed and Energy19. This accreditation will serve as a quality label for certification authorities that satisfy the requirements in annex 2, that provide certificates that comply with the requirements in annex 1, and that use means to create signatures that comply with the requirements in annex 3 of the Certification Services Provider Act.

Finally, a qualified signature is created using a secure signature creation device as

Requirements in annex 3 of the Certification Services Provider Act

- The information used to create a signature must be unique and non-recurrent. Everything possible must be done to ensure the confidentiality of this information.
- The certificate holder must have reasonable certainty that information used to create the signature cannot be derived from the resulting signature or the certificate. The signature should be protected against forgery using currently available technology.
- The certificate holder must be able to protect the data for creating the signature reliably against use by others.
- The qualified electronic signature is not the only legally valid electronic substitute for a handwritten document. The introduction of the electronic signature into the law of evidence is only a small step in the modernization of current law. It can now be drafted and signed on a digital document submitted to him as a signed document.

3.3. SCOPE OF THE NEW REGULATIONS

The introduction of the electronic signature into the law of evidence is only a small step in the modernization of our law. Contracts can now be drafted and signed electronically. If all conditions have been fulfilled, such an electronic contract will have the special evidential value of a privately signed document.
important arguments for the purpose of archiving sufficient evidence of these relatively new and not-yet-drafted versions of agreements, may be replaced by an electronic version of an original document. However, plain electronic documents do not have the special evidential value of original documents.

In certain cases, other formal conditions besides the signature exclude electronic documents. For example, a unilateral promissory note must contain the handwritten phrase "read and approved".

These gaps will gradually be filled in the future. The Electronic Commerce Act, which will be covered later on, has gone part way in this direction. Electronic signatures are still necessary, such as in electronic pre-orders of orders, in electronic contracts of sale, and in electronic acceptance of orders. The term "virtual" is dominated by electronic means from the internet. However, electronic documents have no special evidential value over handwritten and signed documents.

Any type of evidence can be used to substantiate transactions with a value of less than 375 EUR.

4. EXCEPTIONS TO THE SIGNED-DOCUMENT REQUIREMENT:

4.1. COMMENCEMENT OF WRITTEN PROOF

The lack of proper documentary evidence, namely an original signed document, is excusable when one submits other reliable evidence in written form. This mode of proof with all required formalities is called a commencement of written proof in legal jargon. The term "written" must be interpreted broadly: it can mean an irregular authentic act that doesn't comply with all required formalities to be valid, such as a simple letter, a fax, or even an electronic document without any formalities. The parties themselves are responsible for their evidence. The court may decide on the credibility of the evidence. A plain document does not have the special evidential value of a signed document.

Under these circumstances, original paper documents, whether signed or not, which were drafted when entering into the agreement, may be replaced by an electronic version of the original document. But this does not mean that an electronic signature can always replace a hand-written signature.
4.3. FORCE MAJEURE OR “ACT OF GOD”

Similarly, it is not necessary to submit proper documentary evidence when the creditor was unable to procure written evidence due to force majeure or an “act of God” (art. 1348 of the Belgian Civil Code). In some situations, circumstances beyond one’s control prevent the drafting of a document. In other cases, documentary evidence that had been drafted is lost due to an unforeseen accident caused by circumstances beyond one’s control. Evidently, purposely destroying the original evidence to replace it with electronic images does not fall within the scope of this exception.

4.4. COMMERCIAL EVIDENCE LAW

The rules of evidence in commercial law are traditionally more flexible than the civil rules of evidence. Businesses may use any and all types of evidence to substantiate their assertions. The judge determines the credibility of the evidence presented as he sees fit. This unregulated evidence system is based on art. 25 of the Belgian Commercial Code.

In principle, a signed document is never required as evidence between businesses, regardless of whether the value of the transaction exceeds the €3,750 EUR limit. In principle, a signed document is never required as evidence between businesses.

Moreover, businesses are often obliged to store information in paper form for reasons other than the law of evidence. The government exercises control over businesses for economic, social security, tax and other purposes. The way in which this control is exercised frequently implies the use of paper documents. Handwritten and printed evidence is collected through inspection of premises, inspection of documents, inspection of business records, etc. The judge’s task is to determine the credibility of this evidence.

The scope of the commercial rules of evidence is very narrow, and business transactions are concerned only when one of the parties is a private individual. The business partner must thus be able to submit a signed document for transactions having a value in excess of €375 EUR. If the transaction is concluded through electronic means, both parties must place an electronic signature on the electronic document. The judge determines the credibility of the signed document as he sees fit. This arrangement is prompted by the rapid and informal character of business transactions.

Under these circumstances, original paper documents may be replaced by electronic data, e.g. using scanning techniques or microfilm, for archival purposes. The scope of the commercial rules of evidence is very narrow, and business transactions are concerned only when one of the parties is a private individual.
The current requirements of form are not abolished, but it will be possible to fulfill them electronically. The modernization of evidence law is an essential step in achieving the legal framework for business archives. The obligations of the parties to a contract can now also be fulfilled electronically. The parties to a contract are free to use a variety of techniques to sign their documents as long as the attribution and integrity of the signature is guaranteed. The fulfillment of these conditions will be verified by the judge in case of a dispute. The use of a qualified signature is by no means mandatory, but such a signature has the advantage that it is valid throughout the European Union as a substitute for a handwritten signature.

1. ONLINE CONTRACTING

The intention of the Electronic Commerce Act is to remove all obstacles that hinder entering into contracts in relation to a service of the information society. All steps in the process of contract conclusion are addressed from the initial negotiations, over the tender, the signing, the invoicing to the registration and archiving of the contract.

The current requirements of form are not abolished, but it will be possible to fulfill them electronically. The current requirements of form are not abolished, but it will be possible to fulfill them electronically. The current requirements of form are not abolished, but it will be possible to fulfill them electronically.

The intention of the Electronic Commerce Act is to remove all obstacles that hinder entering into contracts in relation to a service of the information society. All steps in the process of contract conclusion are addressed from the initial negotiations, over the tender, the signing, the invoicing to the registration and archiving of the contract.

The current requirements of form are not abolished, but it will be possible to fulfill them electronically. The current requirements of form are not abolished, but it will be possible to fulfill them electronically. The current requirements of form are not abolished, but it will be possible to fulfill them electronically.
Next to the signature, our law contains other formal prescriptions that hinder the conclusion of contracts electronically. Besides several direct obstacles, such as the formal obligation to use paper, there are also many indirect obstacles. Uncertainty exists concerning the application of some procedural requirements on contracts entered into electronically. A few examples are "registered mail sent by the postal services", inclusion of handwritten notices, drafting multiple copies, use of special layout or forms, etc. Frequently, these formal requirements must be satisfied to ensure the validity of the contracts or other legal transactions involved, and not only to constitute evidence, as described in the previous chapter.

The legislator chose not to tackle existing procedural requirements one by one, because such a comprehensive analysis of Belgian law would be too time consuming. Instead, several transversal stipulations were introduced that cut across the entire body of law. In the past, this method was used to introduce the euro into Belgian law.

Art. 16 §1 of the law stipulates that any legal or regulatory requirement of form applicable to the conclusion of contracts is deemed satisfied if the functional qualities of this requirement are fulfilled. In other words, the parties to the contract may develop their own electronic alternative for existing formal requirements. Thus, it is necessary to determine the objective or functional qualities of each formal requirement. This is not a simple task, since most formal requirements do not state the objective they pursue. Similar requirements of form can pursue different objectives depending on the legislation that imposes them. For instance, signatures sometimes serve as evidence and sometimes for the validity of a legal transaction. The contracting parties will only be absolutely certain that the electronic alternative they developed suffices when a judge has confirmed this in the event of dispute.

Art. 16 §2 provides further information regarding formalities that are very common. This is the case for the writing, the signature, and the handwritten notice. Nonetheless, the parties to the contract must perform the same exercise for these three procedural requirements as for any other procedural requirement. Under certain circumstances a writing, a signature or a handwritten notice can have other functional qualities than those explicitly described in the Electronic Commerce Act. A writing is a series of legible signs that must be accessible for later consultation. Moreover, the medium must be durable enough to allow the information stored to be accessible for later consultation. Regarding the signature, we are referred to the rules on the electronic signature in the Belgian Civil Code and the Certification Service Provider Act. The requirement of a signature is fulfilled when the electronic signature satisfies the two conditions set by the evidence rules (identification and integrity) or when the electronic signature is qualified electronic signature (presumption that these two conditions have been fulfilled).

At first glance, it is strange to see a reference here to already-existing regulations governing the electronic signature. The reason is to provide legal recognition beyond the scope of evidence law, whereas the Belgian Civil Code and the Certification Service Provider Act do not affect the legal status of the electronic signature outside the context of contracts. Art. 15 of the law stipulates that any legal or regulatory requirement of form in the conclusion of contracts, whether they are electronic or not, must be satisfied.

Concluding, the conclusion of contracts electronically results in the need for a legal framework that provides for both evidence and the validity of contracts. While the legislation already provides for formal requirements of form, it is necessary to determine the objective or functional qualities of these requirements to ensure that the electronic alternative developed suffices. This requires a comprehensive analysis of the legislation that imposes these requirements, which is time-consuming. The legislator chose not to do this, but rather introduced transversal stipulations that cut across the entire body of law.
The rules of evidence in the Electronic Commerce Act recognize the electronic signature for use in all aspects of the contractual process. From now on, whenever a signature is required in any stage of contract conclusion, an electronic signature is a valid alternative. This is important, for instance, when a signature is needed for the validity of a contract.

Nevertheless, one must bear in mind the limited scope of the law: it affects only formal requirements that impede the conclusion of contracts electronically. For instance, the law does not alter the formal requirements that impede the conclusion of contracts for certain types of contracts. These exceptions will remain until the legislator expressly abolishes them.

2. EXCEPTIONS

The law does not alter the formal requirements that impede the conclusion of contracts for certain types of contracts. These exceptions will remain until the legislator expressly abolishes them.

The following types of contracts are involved:

• The transfer of property rights on real estate, in whole or in part.
• Contracts that fall within the scope of family or inheritance law, for instance nuptial agreements.
• Contracts that must be concluded before a civil law notary or a public official, such as in a notarization.
• The creation of property rights on real estate, in whole or in part.

Although the law does not alter the formal requirements that impede the conclusion of contracts for certain types of contracts, the following exceptions will remain until the legislator expressly abolishes them:

• The transfer of property rights on real estate, in whole or in part.
• Contracts that fall within the scope of family or inheritance law, for instance nuptial agreements.
• Contracts that must be concluded before a civil law notary or a public official, such as in a notarization.
• The creation of property rights on real estate, in whole or in part.
3. COMMERCIAL LAW AT TWO SPEEDS

The formalities proscribed in these cases cannot be replaced with a simple set of transversal stipulations. The law imposes several special guarantees for these contracts, such as the intervention of a third party, the drafting of an inventory, the presence of witnesses, etc. These guarantees must neither be applied to all of the contracts considered as part of a transaction related to a service of the information society, as a consequence of this, important to keep in mind that these formalities are only taught for commercial purposes.

The Electronic Commerce Act removes several of the remaining legal obstacles to the conclusion of contracts electronically. The parties to the contract are granted a great degree of uncertainty concerning the legal validity of the procedures they have developed. These procedures still need to be adapted to the paper world to develop their own electronic procedures for the formal requirements they have created. For the paper world, the formal requirements that were created for the paper world to develop their own electronic procedures for the formal requirements that were created for the paper world.

The Electronic Commerce Act removes several of the remaining legal obstacles to the conclusion of contracts electronically. The parties to the contract are granted a great degree of uncertainty concerning the legal validity of the procedures they have developed. These procedures still need to be adapted to the paper world to develop their own electronic procedures for the formal requirements they have created. For the paper world, the formal requirements that were created for the paper world to develop their own electronic procedures for the formal requirements that were created for the paper world.

The Electronic Commerce Act removes several of the remaining legal obstacles to the conclusion of contracts electronically. The parties to the contract are granted a great degree of uncertainty concerning the legal validity of the procedures they have developed. These procedures still need to be adapted to the paper world to develop their own electronic procedures for the formal requirements they have created. For the paper world, the formal requirements that were created for the paper world to develop their own electronic procedures for the formal requirements that were created for the paper world.

The Electronic Commerce Act removes several of the remaining legal obstacles to the conclusion of contracts electronically. The parties to the contract are granted a great degree of uncertainty concerning the legal validity of the procedures they have developed. These procedures still need to be adapted to the paper world to develop their own electronic procedures for the formal requirements they have created. For the paper world, the formal requirements that were created for the paper world to develop their own electronic procedures for the formal requirements that were created for the paper world.
1. ACCOUNTING OBLIGATIONS

The purpose of keeping accounts is to provide the company and third parties with a realistic and complete picture of the company’s assets, financial situation, and results. In Belgian law, the Accounting Act is more flexible when it comes to documents that provide information supporting the books. These documents may be exchanged in electronic form, as long as they comply with the law’s requirements.

The Accounting Act is more flexible when it comes to documents that provide information supporting the books. These documents may be exchanged in electronic form, as long as they comply with the law’s requirements.

According to Article 5 of the Accounting Decree, the most important ledgers must be stamped by the clerk of the commercial court holding the trade register where the company is located. The law lists the ledgers concerned, specifically the cash received ledger, the central ledger, and the inventory ledger. The company may keep bound registers made in accordance with an approved model. If a company works with loose sheets, the clerk must put a stamp or sign his initials on each sheet. From the wording of the Accounting Decree, it appears that it is presumed that the ledgers are kept manually on paper. For this reason, only the paper version of the most important ledgers is considered legally valid.

Other parts of the accounting books, such as the subsidiary journal, need not be stamped or signed and may thus be kept on any other suitable material. An electronic version can also be legally valid. A condition for this is compliance with the general principles set out in Article 7 §2 of the Accounting Act. More specifically, there must be certainty that the entries cannot be modified once entered. This principle applies to both traditional, manual bookkeeping systems and automated bookkeeping systems.

Accounting software or systems must be designed in such a way that a definitive entry can only be changed by a counter-entry. The original entry must also always remain visible. This principle applies to both traditional, manual bookkeeping systems and automated bookkeeping systems. Modernization of the accounting system is more advanced when it comes to invoicing and tax submission. However, the submission of annual accounts is more traditional. In this domain, the submission of annual accounts is still largely oriented toward a paper accounting system, which continues to be widely used in Belgium. Nevertheless, the law has evolved to accommodate electronic submission. The accounting act is nearly thirty years old and was written when the only acceptable form of communication was paper. The law must also evolve with the technological developments to ensure that all processes, including the submission of annual accounts, are transparent and accurate.

The purpose of keeping accounts is to provide the company and third parties with a realistic and complete picture of the company’s assets, financial situation, and results. If a company needs to keep accounts, it must do so in a manner that is consistent with the law.
2. ACCOUNTING AND TAX LAW

The ledgers must be stored for ten years starting from the first of January of the year following that in which they were closed. This long retention period imposes a heavy burden on companies, as physical storage space is usually quite costly. To accommodate this, the legislator allows the unstamped ledgers to be kept either in the original form (on paper or electronically) or as copies. The original unstamped paper ledgers, where applicable, may then be destroyed. The stamped books, by contrast, must still be stored in the original paper version.

The supporting documents must also be stored for ten years. This period is reduced to three years when they cannot serve as evidence against third parties. These documents may be stored in original form (on paper or electronically) or as copies. The original paper accounting documents may be scanned and stored in digital form. The paper original may then be destroyed.

The tax authorities also have an interest in the accounts. The legislation on income tax and the VAT regulations both impose obligations regarding maintaining and preserving books. Sometimes these rules diverge from those of accounting law. As far as income tax is concerned, the taxpayer is obliged to store all ledgers and records that can be used to determine the amount of taxable income. The tax authorities can demand this information up to the end of the fifth year following the taxable year. For the VAT, art. 60 of the VAT Act sets the storage period for ledgers and records at ten years.

Traditionally, tax law adopts a more pragmatic attitude than does accounting law. The tax authorities' sole aim is an accurate tax levy, which results in a less formalistic approach: the content of the accounts is more important than their form. There is no question of a stringent regulation of the form which the accounts must take. An accounting system that does not comply with all the formalities of accounting may still have evidential value for tax purposes.

The tax payer must be able to present to the revenue service the mandatory ledgers and documents, such as the receipt books required by article 320 of the Income Tax Code, the documents that have served for keeping accounts and in general all documents that can be useful in determining the taxable base. For the VAT purposes, the accounts consist of the following ledgers: a ledger for incoming invoices, a ledger for outgoing invoices and a journal in which receipts are entered in which receipts are entered. The supporting documents consist of the following ledgers and records: a ledger for incoming invoices, a ledger for outgoing invoices and a journal in which receipts are entered.

Traditionally, tax law demands that the tax authorities be able to present the tax law. The tax authorities also demand that the ledgers and records be presented in a legible and comprehensible form. The tax officials may demand copies of electronic ledgers and records in a form of their choice. Finally, they require the tax payer to keep the original ledgers and records, as per article 320 of the Income Tax Code.
can request the taxpayer to repeat his calculations to ensure that the correct tax is levied. This last obligation has far-reaching consequences. The bookkeeping must not only be preserved, it must be preserved in such a way that calculations can be performed with the data. This obligation entails a considerable extra cost for companies that keep their accounts electronically. The company can opt to preserve the computer system in which the books and records were created in operational condition. However, maintaining an obsolete computer system for a long period is far from obvious. The cost of maintenance and replacement parts can be high. Moreover, in some cases the company will have replaced its accounting system more than once during the mandatory retention period. A second option is to migrate all the accounts to the new accounting system, provided that there are sufficient guarantees that the books will remain unaltered.

As is the case in accountancy law, the regulation on income tax and VAT requires, in principle, that all original paper documents be preserved. As an exception, the income tax and VAT authorities allow certain ledgers and records to be stored on microfilm, micro cards or CD-WORM. The ledgers and records involved include the following:

- The duplicates of documents drafted by the taxpayer and correspondence that was not supplemented or signed by the addressee, with the exception of any documents bearing an official seal or any other mark required by tax regulations. The copies of outgoing invoices may be scanned then destroyed. Original purchase invoices, bank statements, receipts and duplicates of VAT slips that restaurants are required to provide to their customers are excluded from this regulation. Any document to which an invoice refers for the description of the delivered goods or services, such as the contract or the delivery note, must be preserved under the same conditions as the incoming invoice.

- The ledgers and registers prescribed by the VAT Act, with the exception of the receipts journal. The ledgers for incoming invoices and the ledger for outgoing invoices may not be replaced by microfilm or micro cards for retention purposes when they are among the ledgers stamped in accordance with the Accounting Act.

- The ledgers and registers prescribed by the VAT Act, with the exception of the receipts journal. The ledgers for incoming invoices and the ledger for outgoing invoices may not be replaced by microfilm or micro cards for retention purposes when they are among the ledgers stamped in accordance with the Accounting Act.

- The conditions for storage on microfilm or micro card are the same for both income tax and VAT. The most important are:
  - Outgoing invoices must be stored on film, card or CD-WORM in the order of their registration in the outgoing invoice ledger. The other documents must be stored in chronological or numerical order.
  - Each film, card or CD-WORM may only contain one book or one particular type of document.
  - The ledgers and registers must be preserved under the same conditions as the incoming invoice. The ledgers and registers prescribed by the VAT Act with the exception of the receipts journal may not be replaced by microfilm or micro cards for retention purposes when they are among the ledgers stamped in accordance with the Accounting Act.

- The condition for storage on microfilm or micro card is that all original paper documents be preserved. As an exception, the income tax and VAT authorities allow certain ledgers and records to be stored on microfilm, micro cards or CD-WORM. The most important are:
  - Outgoing invoices must be stored on film, card or CD-WORM in the order of their registration in the outgoing invoice ledger. The other documents must be stored in chronological or numerical order.
  - Each film, card or CD-WORM may only contain one book or one particular type of document.
  - The ledgers and registers must be preserved under the same conditions as the incoming invoice. The ledgers and registers prescribed by the VAT Act with the exception of the receipts journal may not be replaced by microfilm or micro cards for retention purposes when they are among the ledgers stamped in accordance with the Accounting Act.

- The condition for storage on microfilm or micro card is that all original paper documents be preserved. As an exception, the income tax and VAT authorities allow certain ledgers and records to be stored on microfilm, micro cards or CD-WORM. The most important are:
  - Outgoing invoices must be stored on film, card or CD-WORM in the order of their registration in the outgoing invoice ledger. The other documents must be stored in chronological or numerical order.
  - Each film, card or CD-WORM may only contain one book or one particular type of document.
  - The ledgers and registers must be preserved under the same conditions as the incoming invoice. The ledgers and registers prescribed by the VAT Act with the exception of the receipts journal may not be replaced by microfilm or micro cards for retention purposes when they are among the ledgers stamped in accordance with the Accounting Act.

- The condition for storage on microfilm or micro card is that all original paper documents be preserved. As an exception, the income tax and VAT authorities allow certain ledgers and records to be stored on microfilm, micro cards or CD-WORM. The most important are:
  - Outgoing invoices must be stored on film, card or CD-WORM in the order of their registration in the outgoing invoice ledger. The other documents must be stored in chronological or numerical order.
  - Each film, card or CD-WORM may only contain one book or one particular type of document.
  - The ledgers and registers must be preserved under the same conditions as the incoming invoice. The ledgers and registers prescribed by the VAT Act with the exception of the receipts journal may not be replaced by microfilm or micro cards for retention purposes when they are among the ledgers stamped in accordance with the Accounting Act.

- The condition for storage on microfilm or micro card is that all original paper documents be preserved. As an exception, the income tax and VAT authorities allow certain ledgers and records to be stored on microfilm, micro cards or CD-WORM. The most important are:
  - Outgoing invoices must be stored on film, card or CD-WORM in the order of their registration in the outgoing invoice ledger. The other documents must be stored in chronological or numerical order.
  - Each film, card or CD-WORM may only contain one book or one particular type of document.
  - The ledgers and registers must be preserved under the same conditions as the incoming invoice. The ledgers and registers prescribed by the VAT Act with the exception of the receipts journal may not be replaced by microfilm or micro cards for retention purposes when they are among the ledgers stamped in accordance with the Accounting Act.
Although this solves a part of the storage problem, the scope of this exemption is limited. The requirement to preserve the originals still remains for many items of evidence. Moreover, the solutions offered aren’t very flexible, as the administration only accepts certain technologies. The technological evolution has not slowed its pace and the CD-WORM is gradually becoming obsolete due to the rise of the DVD-WORM and software-based WORM solutions. These are two basic types of systems involving the CD-WORM and involving the WORM technology. Various e-invoicing platforms have been developed on the market for several years. However, the lack of a uniform framework in the European Union hindered the electronic invoicing processes.

Until recently, the lack of a uniform framework in the European Union hindered the electronic invoicing processes. The European Union issued Directive 2001/115 on the harmonization of invoicing rules on January 28, 2001. The directive aimed to eliminate these and other invoicing bottlenecks. In addition, the directive created a uniform legal framework for electronic invoicing and electronic trade, thus contributing to the harmonization of invoicing rules. The European Communities governing self-billing and the outsourced procedures.

The technology to exchange invoices electronically has been around for several years. Companies are very interested in the savings this could bring, and the tax authorities are also gradually discovering numerous advantages to the electronic invoice. Research has shown that the cost of a paper invoice lies somewhere between €1.13 and €1.65 EUR, against €0.28 to €0.47 EUR for an e-invoice. Electronic invoicing is a logical step in the increasing automation of business processes.

Until recently, the lack of a uniform framework in the European Union hindered the electronic invoicing processes. The European Union issued Directive 2001/115 on the harmonization of invoicing rules. The directive aimed to eliminate these and other invoicing bottlenecks. In addition, the directive created a uniform legal framework for electronic invoicing and electronic trade, thus contributing to the harmonization of invoicing rules. The European Communities governing self-billing and the outsourced procedures.

Various e-invoicing platforms have been available on the market for several years. There are two basic types of systems involving the CD-WORM and the WORM technology. These are two basic types of systems involving the CD-WORM and involving the WORM technology. Various e-invoicing platforms have been developed on the market for several years. However, the lack of a uniform framework in the European Union hindered the electronic invoicing processes.

The invoice is one of the most important items of evidence in accounting. The invoice is one of the most important items of evidence in accounting. The invoice is one of the most important items of evidence in accounting. The invoice is one of the most important items of evidence in accounting.
In principle, the supplier of goods or services is obliged to draft an invoice for every delivery that he makes. He can also opt to mandate his customer or a third party to draft the invoice in his name. Even though the concept “invoice” was not defined in the Belgian VAT Act, the tax authorities used to presuppose that an invoice was necessarily a paper document. Exceptionally, the tax authorities granted certain companies a license to invoice electronically. Since 1 January 2004, electronic invoicing is open to everyone, insofar as the legal conditions are respected. First of all, the other party to the contract must be willing to accept an electronic invoice. This acceptance can be expressed either explicitly or implicitly. In addition, the authenticity and integrity of the invoice must be guaranteed. To achieve this, the person issuing the invoice can use two techniques: either he signs the invoice with a secure electronic signature, or he sends the invoice in accordance with the “EDI-standard code.”

The concept “secure electronic signature” is synonymous with the advanced electronic signature referred to in the Certification Services Provider Act. A qualified certificate is not required. Although the term “signature” is used, this is not a signature in the legal sense. After all, the Directive states that the Member States may not ask that the invoice be signed. In this context, the concept “secure electronic signature” refers exclusively to the technical notion. The term “electronic stamp” would perhaps have been more suitable.

The concept “EDI-standard code” does not refer to an official EDI standard, such as UN/EDIFACT, but to the message structure to which the parties have agreed. In each case, the EDI procedures that have been agreed upon must guarantee the authenticity of the origin of the invoice and the integrity of the data.

In principle, a simple e-mail does not suffice as a valid invoice. Nevertheless, the Ministry of Finance has the right to accept a normal e-mail and even other methods of electronic invoicing insofar as the authenticity and integrity are guaranteed.

The directive forbids Member States from imposing more stringent conditions, except for invoices originating in a country outside the EU for goods or services delivered in Brussels.

An invoice must always be drafted in duplicate. The original copy is intended for the customer, while the person registered for VAT must store a copy. Article 60 of the Belgian VAT Act imposes the obligation on both the person registered for VAT and the customer to preserve copies of the invoices for ten years. Nevertheless, the authorities accept that the customer – when a natural person purchasing goods or services intended for private use and to whom an invoice was still delivered – must only store the invoice for five years.

Paper invoices must be stored in Belgium. Thus ensuring easy access for inspection.

For the years preceding 2004, invoices were still delivered – must only store the invoice for five years. The directive, however, does not mention this directive explicitly. In practice, member states may ask their citizens to store invoices for longer periods. The Belgian VAT Act does not mention the requirements for stored invoices. The authorities accept that the digital archives can be stored anywhere in Europe if the taxpayer notifies them beforehand. The authorities must receive access to the invoices stored in another Member State (Article 61, §1, par. 2 of the Belgian VAT Act).
Digital archiving

Part 1: The Legal Framework for Business Archives

...stipulates that this should be allowed when there are administrative agreements with the non-member country in question59. The customer must store his original invoice in the form in which it was received, be it on paper or electronically 60. He can only exercise his right to deduct VAT paid when he can submit an original invoice. The supplier may preserve his copy of the paper invoice on microfilm, micro card or CD-WORM and destroy the paper copy. The authenticity of the origin and the integrity of the content of the invoice as well as its legibility must be guaranteed throughout the entire retention period. Moreover, the information that guarantees the authenticity and the integrity of the electronic invoice must also be preserved61.

The new legal stipulations give companies greater freedom to adapt their invoicing procedure to their needs. The law limits itself to establishing the objectives that an invoice must meet and is formulated in a technologically neutral manner. This procedure must largely protect the legislative framework from obsolescence due to the rapid evolution in technology. Unfortunately, the executory decrees restrict the freedom offered again to a great degree. As such, both EDI and the secure signature allow a broad scale of implementations, yet several other procedures are excluded a priori. It is to be hoped that the Finance Minister will remove these restrictions again in the near future.

4. PUBLICATION OF THE ANNUAL FINANCIAL STATEMENT

In addition to maintaining regular accounts, companies must submit an annual financial statement each year to the National Bank of Belgium (NBB). This statement must include a statement of assets and liabilities, a statement of earnings and the notes to the financial statements. For financial statements drafted integrally in accordance with either the full scheme or the abbreviated scheme63, the submitter may choose to transmit the documents in an electronic form, either by handing over a diskette or via the internet, or may choose to submit them on paper. Exceptionally, the annual financial statement must still be presented on paper when it is drafted in a currency other than the euro or when some headings in the statement were adapted to the special nature of the company's activities.

The Central Balance Sheet Office publishes the technical specifications that financial statements submitted on diskette must satisfy in the “Protocol for Submitting Annual Financial Statements on Diskette”. Various companies use this protocol when developing software to draft annual financial statements. Alternatively, the person required to submit the statement can download a free submission program from the National Bank of Belgium. Submission through the internet is not yet available to all companies. For the time being companies must submit financial statements over internet. Only third-party submitters who submit many financial statements over internet can participate in the pilot project. It is hoped that the pilot project will be opened to all standardized financial statements in the course of 2005. The company must already have performed the arithmetic and logical verification.
of the annual financial statement before submitting it in electronic form. The National Bank examines the annual financial statements submitted on paper. Each annual financial statement must be placed on a separate diskette or in a separate electronic message. The lower fee that applies to electronic submission is intended to stimulate its uptake.

5. PAPER LOSES GROUND

THE LAW REGULATES EMPLOYERS TO MAINTAIN SOCIAL DOCUMENTS SO THAT IT CAN BE DETERMINED AT ANY MOMENT WHICH EMPLOYEES WORK FOR A GIVEN EMPLOYER. THE OBJECTIVE IS TO PROVIDE ELECTRONIC INVOICES.

Greatest progress occurred in the area of invoicing. Prompted by the European Union, all Member States developed a similar legal framework for the exchange of electronic invoices. GeoLink is open to all companies, but in the future submission over the internet will be mandatory. The annual financial statement may be submitted electronically. As this means more accounts on paper, certain documents may be converted from paper to electronic form. This may include the following accounts:

- General and special personnel registers
- Written employment contracts for the employment of students and apprentices
- Domestic servants
- The annual financial statement of a person
- Social documents
- The general and special personnel registers
- The individual account
- The annual financial statement of a person

Already in 1986 employers were required to maintain a personnel register. Today, the regulations governing social documents can be found in Royal Decree no 5 of 23 October 1978. The Royal Decree lists the social documents:

- General and special personnel registers
- The annual financial statement of a person

1. WHAT ARE SOCIAL DOCUMENTS

6. SOCIAL DOCUMENTS

Electronic invoices are exchanged between companies, and the law regulates the maintenance of accounts. The annual financial statement must be placed on a separate diskette or in a separate electronic message. The National Bank examines the annual financial statement submitted in electronic form. The National Bank examines the annual financial statement submitted in electronic form.
3. FORM AND RETENTION PERIOD

OF SOCIAL DOCUMENTS

Two periods in time must be distinguished in order to know what form the social documents must take. Up to a certain point, the social documents are being exempt from the obligation to keep social documents. Employers employing foreign workers within the territory of Belgium are also partly exempt from the obligations of keeping social documents. By a circular of 21 March 2006, the employment and social security authorities have stated that social documents, such as the personnel register, the individual account and the attendance register, are subject to social security surveillance, even if the documents are only required or used for administrative purposes.

Section 1

2. WHO IS OBLIGED TO KEEP SOCIAL DOCUMENTS

The personnel register is a register in which all employees are registered in chronological order of the commencement of their employment. In principle, the employer must maintain one personnel register for all his employees. Separate registers for white-collar and blue-collar workers are not allowed. The special register is only required when the employer has people working at more than one location. In this case, a separate personnel register is kept at each location.

The individual account is a detailed description of the work an employee has performed for his employer during a given year. It also states the days worked, the days not worked, the elements that make up the salary and the deductions from it (social security, income tax, etc). The individual account also contains all useful administrative information in relation to the salary (for instance, the joint committee, the employer’s salary administration service, etc.).

The attendance register records the employees’ presence. This regulation only applies to a few industries, such as the diamond, the hospitality, the agricultural and the truck farming industries.

Special rules apply to keeping social documents for dockworkers. Special rules are planned for unemployed persons assigned a place in a community work scheme.

Royal Decree no. 5 has a broad scope of applicability and applies to all employers and the self-employed, with the exception of the following:

• persons who perform work under the authority of another person even when there is no employment contract (for instance, inmates assigned work)
• persons who fall partially or completely under the social security legislation and whose activities are not included in an employment contract
• persons who perform work under the authority of another person even when there is no employment contract (for instance, inmates assigned work)

The law of 3 July 1998 (Employment Contract Act) applies to the employer who hires a student or home worker to draft a written employment contract containing several clauses. An analogous obligation applies to an apprentice contract for part-time pupils.

The law of 3 July 1998 (Employment Contract Act) applies to the employer who hires a student or home worker to draft a written employment contract containing several clauses. An analogous obligation applies to an apprentice contract for part-time pupils.

The law of 3 July 1998 (Employment Contract Act) applies to the employer who hires a student or home worker to draft a written employment contract containing several clauses. An analogous obligation applies to an apprentice contract for part-time pupils.

• persons who perform work under the authority of another person even when there is no employment contract (for instance, inmates assigned work)
• persons who fall partially or completely under the social security legislation for employees (e.g. professional soccer players)
• apprentices

Civil servants employed by the federal government, by federations and agglomerations of municipalities, by provinces and by municipalities are not considered employees for the application of the regulations governing social documents. Employers employing foreign workers within the territory of Belgium are also partly exempt from the obligation to keep social documents. By a circular of 21 March 2006, the employment and social security authorities have stated that social documents, such as the personnel register, the individual account and the attendance register, are subject to social security surveillance, even if the documents are only required or used for administrative purposes.

Section 2

3. FORM AND RETENTION PERIOD

OF SOCIAL DOCUMENTS
3.1. MAINTAINING SOCIAL DOCUMENTS

The form in which the general and special personnel registers, the individual account, the apprentice contract for part-time pupils, the employment contract for students and domestic servants must be maintained is regulated in the Royal Decree of 8 August 1980 on keeping social documents (Moniteur belge, 27 August 1980).

The personnel register must be kept in the form of a bound book with consecutively numbered pages. It may consist of several bound books if lack of space prevents the required information from being recorded on a previous volume. In that case the page and employee numbers must continue in subsequent volumes (art. 4 §2 of the Royal Decree of 8 August 1980).

The special personnel register may be kept on a paper or electronic medium on the condition that it is easy to read and that the reproduction permits efficient inspection (art. 11 §2, par. 2 of the Royal Decree of 8 August 1980). There are no further formal requirements.

There is no regulated form for the individual account or for the employment contract for students and domestic servants. The same applies to the apprentice contract for part-time pupils. The employer may establish his own form. The document must contain all the mandatory information. The employer must provide the employee with a copy of the individual account before the first of March of the following year.

A Royal Decree of 17 June 1994 (Moniteur belge 25 June 1994) stipulates the form of the attendance register. In principle, it consists of bound and consecutively numbered monthly sheets. It must be drafted by calendar year. The list of those present at work must be legible and recorded in indelible ink (art. 4 §2 of the Royal Decree of 17 June 1994). The blank attendance registers must be certified and delivered by the body indicated for the purpose in the regulations specific to the industry sector in question.

3.2. PRESERVING SOCIAL DOCUMENTS

The employer may preserve social documents in original form or in any kind of reproduction on the condition that it is easy to read and that the reproduction permits efficient inspection (art. 17 §2, par. 2 of the Royal Decree of 8 August 1980). The storage period is 5 years starting from:

- the date that the last mandatory information was recorded for the general personnel register
- the date the agreement ends for the individual account
- the day following the day after the execution of the contract ends for the employment contract for students
- the date that the last mandatory information was recorded for the attendance register

The retention period is not explicitly mentioned for employment contracts for students and domestic servants.
4. IMMEDIATE NOTIFICATION REGARDING EMPLOYMENT (DIMONA)

DOMESTIC SERVANTS AND THE APPRENTICE CONTRACT FOR PART-TIME PUPILS.
The rule applicable to the employment contract for students can be followed by analogy.

The employee can ask to be paid on the basis of the guarantee. The employee is entitled to
manual deploring the fields of the employment contract, and to perform the
persons in the company responsible for developing the application can consult the

The Dimona notification must reach the national office of Social Security (RSZ)

The Dimona notification was made obligatory on 1 January 1999 in the passenger transport, temporary employment and construction industries. The immediate notification of employment was made obligatory on 1 January 2003. The Dimona notification must reach the Social Security Administration in the form of an electronic message. Employers who do not have internet access can send their notification to the RSZ by using a voice server accessible by telephone. The questions presented can be answered by pressing the telephone buttons. The social security administration can then send the notification to the RSZ along with a number of attached documents or electronic messages.

The employer can report the hiring of an employee to various social security institutions, such as the child benefit institution, the industrial injuries insurer, an institute for the payment of vacation pay, etc. In addition, the social security administration often requests certain information from the employer. Although these institutions all require similar information, they use different forms of application for the same information.

To cut down on all this paperwork, the program law of 26 July 1996 provided for a modernization of the social security system and a simplification of the social administration. The objective of the "Déclaration IMMédiate or in Dutch ONmiddellijke Aangifte" (Dimona [Immediate Notification]) is to provide immediate notification of the commencement and termination of employment to those government institutions that need it. In the future, the immediate notification must facilitate the various social security institutions' ability to consult the Crossroads Bank for Social Security (a database for electronic data exchange) and have access to the information relevant for social legislation.

The immediate notification of employment was made obligatory on 1 January 1999 in the passenger transport, temporary employment and construction industries. The Dimona notification must reach the National Office of Social Security (RSZ) in the form of an electronic message. Employers who do not have internet access can send their notification by using a voice server accessible by telephone. The questions presented can be answered by pressing the telephone buttons. The social security administration can then send the notification to the RSZ along with a number of attached documents or electronic messages.

The employer can also call in one of the agencies that provide support in fulfilling social security obligations (salary administration services, software developers). They act as intermediaries in submitting the Dimona notification. They provide various services, such as administration of Social Security Services, software development, and consulting.

The employee can ask to be paid on the basis of the guarantee. The employee is entitled to
manual deploring the fields of the employment contract, and to perform the
persons in the company responsible for developing the application can consult the

The Dimona notification must reach the national office of Social Security (RSZ)

The Dimona notification was made obligatory on 1 January 1999 in the passenger transport, temporary employment and construction industries. The immediate notification of employment was made obligatory on 1 January 2003. The Dimona notification must reach the Social Security Administration in the form of an electronic message. Employers who do not have internet access can send their notification to the RSZ by using a voice server accessible by telephone. The questions presented can be answered by pressing the telephone buttons. The social security administration can then send the notification to the RSZ along with a number of attached documents or electronic messages.

The employer can report the hiring of an employee to various social security institutions, such as the child benefit institution, the industrial injuries insurer, an institute for the payment of vacation pay, etc. In addition, the social security administration often requests certain information from the employer. Although these institutions all require similar information, they use different forms of application for the same information.

To cut down on all this paperwork, the program law of 26 July 1996 provided for a modernization of the social security system and a simplification of the social administration. The objective of the "Déclaration IMMédiate or in Dutch ONmiddellijke Aangifte" (Dimona [Immediate Notification]) is to provide immediate notification of the commencement and termination of employment to those government institutions that need it. In the future, the immediate notification must facilitate the various social security institutions' ability to consult the Crossroads Bank for Social Security (a database for electronic data exchange) and have access to the information relevant for social legislation.

The immediate notification of employment was made obligatory on 1 January 1999 in the passenger transport, temporary employment and construction industries. The Dimona notification must reach the National Office of Social Security (RSZ) in the form of an electronic message. Employers who do not have internet access can send their notification by using a voice server accessible by telephone. The questions presented can be answered by pressing the telephone buttons. The social security administration can then send the notification to the RSZ along with a number of attached documents or electronic messages.

The employer can also call in one of the agencies that provide support in fulfilling social security obligations (salary administration services, software developers). They act as intermediaries in submitting the Dimona notification. They provide various services, such as administration of Social Security Services, software development, and consulting.

An employer must report the hiring of an employee to various social security insti-

tions.

DOCUMENTS FOR A GIVEN PERIOD (ART. 2 Royal Decree no. 5).

The employer must report the hiring of an employee to various social security insti-

tions.

AN EMPLOYER MUST REPORT THE HIRING OF AN EMPLOYEE TO VARIOUS SOCIAL SECURITY INSTI-
TIONS.
An automatic receipt is sent for each Dimona notification. The result of the notification can be consulted on the social security portal site. The employer must store all the messages that he receives from the RSZ for six months.

One consequence of a correct Dimona notification is that the employer no longer has to satisfy several obligations relating to the storage of social security documents. For instance, the general personnel register need no longer be updated. The Dimona notification replaces each new entry in the register. Of course, the old register must still be preserved. The employer also need no longer send a copy of the employment contract for students to the labor inspection.

The e-government platform developed under the direction of the National Office of Social Security and the Crossroads Bank for Social Security is regularly expanded with new applications. It is already possible to submit part of the notification of social risks in electronic form. As of 1 January 2003, the quarterly statement of salary and work time data can only be submitted electronically. The notification for the National Employment and Placement Service (RVA) that an employment contract has been suspended can also be submitted electronically. This involves the suspension of the employment contract for reasons of technical disorder, poor weather or lack of work due to economic causes as regulated respectively in articles 49, 50 and 51 of the Employment Contract Act.

5. OTHER OBLIGATIONS

In addition to social documents, the employer must preserve several other documents. The most important are described in the following paragraphs.

A copy of the part-time employment contract must be kept with the work rules. The employee and employer must both sign this document. In case of a variable work schedule, the daily work schedule for each part-time employee must be posted at least one week in advance and kept on the floor of the company. A copy of the part-time employment contract must be kept with the work rules for one year starting from the day on which the work schedule no longer applies. The employer must store the documents for the whole period that the employee has worked for the company, even after the end of the contract.

The company’s occupational health service must store the medical file of each employee for fifteen years from the time that the employee leaves the company. This file must be kept in a sturdy folder that can be closed on all sides. The personal details of the employee may only be visible on the outside. The folder must also be kept secure. The employer must not store copies of the folders. The company’s occupational health service must store the medical file of each employee for fifteen years starting at the time that the employee leaves the company.
6. TOWARD AN ELECTRONIC SOCIAL FILE

Social security law has already come a long way in its evolution from a paper to an electronic social file. This development started in the administration, with the establishment of the Crossroads Bank for Social Security, and is now gradually being expanded to cover employer-employee relations. The Belgian Medical Assistance and Social Security, for example, has created a medical file for each patient that includes all medical data. This file is not only used for the purpose of treatment, but also serves as evidence in disputes about health care liability and is a source of information for academic research. In practice, there are great differences in the way medical files are handled and maintained.

The medical file has three functions: it is an important tool for the doctor, it serves as evidence in disputes about medical liability, and it is also a source of information for academic research. A medical file is not only used for the purpose of treatment, but also serves as evidence in disputes about medical liability and is a source of information for academic research.

The medical file has three functions: it is an important tool for the doctor, it serves as evidence in disputes about health care liability and is a source of information for academic research. In practice, there are great differences in the way medical files are handled and maintained.

The medical file has three functions: it is an important tool for the doctor, it serves as evidence in disputes about health care liability and is a source of information for academic research.

In the relationship between a doctor and his patient, a great amount of data is generated: information that the patient gives to the doctor, measurements taken by the doctor, x-rays from a radiologist, the results of blood tests, etc. It is of vital importance for the quality of health care that all health professionals maintain a reliable medical file on each patient. Efficient communication of all this data between general practitioners and other health care practitioners is indispensable in optimizing the quality, coherence and continuity of care.

Many laws and rules refer to the notion "medical file":

- Art. 9 §1 of the Patients' Rights Act of 22 August 2002 (Moniteur belge 26 September 2002) gives the patient the right to a conscientiously maintained and securely stored patient file.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) stipulates that a medical file must be created for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.
- Art. 38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical file for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) stipulates that a medical file must be created for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.
- Art. 38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical file for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) stipulates that a medical file must be created for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.

The term "medical file" is not defined clearly anywhere. The law just imposes certain obligations to create a medical file and describes what it must contain. The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.

The medical file has three functions: it is an important tool for the doctor, it serves as evidence in disputes about health care liability and is a source of information for academic research.

In the relationship between a doctor and his patient, a great amount of data is generated: information that the patient gives to the doctor, measurements taken by the doctor, x-rays from a radiologist, the results of blood tests, etc. It is of vital importance for the quality of health care that all health professionals maintain a reliable medical file on each patient. Efficient communication of all this data between general practitioners and other health care practitioners is indispensable in optimizing the quality, coherence and continuity of care.

Many laws and rules refer to the notion "medical file":

- Art. 9 §1 of the Patients' Rights Act of 22 August 2002 (Moniteur belge 26 September 2002) gives the patient the right to a conscientiously maintained and securely stored patient file.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) stipulates that a medical file must be created for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.
- Art. 38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical file for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.
- Art. 38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical file for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.
- Art. 38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical file for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.

The term "medical file" is not defined clearly anywhere. The law just imposes certain obligations to create a medical file and describes what it must contain. The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.

The medical file has three functions: it is an important tool for the doctor, it serves as evidence in disputes about health care liability and is a source of information for academic research.

In the relationship between a doctor and his patient, a great amount of data is generated: information that the patient gives to the doctor, measurements taken by the doctor, x-rays from a radiologist, the results of blood tests, etc. It is of vital importance for the quality of health care that all health professionals maintain a reliable medical file on each patient. Efficient communication of all this data between general practitioners and other health care practitioners is indispensable in optimizing the quality, coherence and continuity of care.

Many laws and rules refer to the notion "medical file":

- Art. 9 §1 of the Patients' Rights Act of 22 August 2002 (Moniteur belge 26 September 2002) gives the patient the right to a conscientiously maintained and securely stored patient file.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) stipulates that a medical file must be created for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.
- Art. 38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical file for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.
- Art. 38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical file for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.
- Art. 38 of the Medical Code of Ethics stipulates that, in principle, the doctor must keep a medical file for each patient.
- The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.

The term "medical file" is not defined clearly anywhere. The law just imposes certain obligations to create a medical file and describes what it must contain. The Royal Decision of 3 May 1999 on the General Medical File (Moniteur Belge 20 May 1999) requires every patient to have a medical file managed by a general practitioner.
2. PRESERVATION PERIOD

The law provides no uniform rules regarding the preservation period for medical files. Each doctor must be able to convince the judge that the data are real and not falsifications. Regardless of the form of the medical file, it must be presented in its original form. Holding prehistoric (prehistoric or ancient) medical records in a secure environment systemizes the need for regulation which states that the medical file is subject to the non-inference of digital archives.

In principle, contractual obligations and other personal actions now expire after 10 years. It is quite possible for a doctor to make an error when treating a patient that cannot be considered a failure to fulfill his contractual obligations. In such cases, claims for compensation for damages based on the doctor's extra-contractual liability expire after five years. However, this term only starts when the patient learns of the damage and the identity of the doctor responsible for the damage. In any event, this claim expires twenty years after the treatment. If the patient was a minor when the error occurred, all these periods commence only when he/she reaches majority. In extreme cases, the period of limitation can span 38 years. Additionally, the doctor may also be subject to criminal prosecution for involuntary assault and battery. In that case, the patient can still submit a claim even if the medical record has been destroyed. If the patient can show reasonable grounds for the destruction of the record, the claim is not barred.

Some actions cause a running term of limitation to be suspended or to be restarted. In practice, it is often difficult to ascertain how long medical documents could be useful as evidence in questions of liability. It can take years for the adverse consequences of a medical error to appear. Preserving a medical file for 30 years will suffice in many cases. Thus, modern alternatives such as destroying the file immediately after the treatment is over can be meaningful. In practice, it means that the file cannot be unambiguously ascertained. Hence, the doctor is faced with the dilemma of deciding how long the file should be preserved.

In principle, contractual obligations and other personal actions now expire after 10 years. It is possible for a doctor to make an error when treating a patient that cannot be considered a failure to fulfill his contractual obligations. In such cases, claims for compensation for damages based on the doctor's extra-contractual liability expire after five years. However, this term only starts when the patient learns of the damage and the identity of the doctor responsible for the damage. In any event, this claim expires twenty years after the treatment. If the patient was a minor when the error occurred, all these periods commence only when he/she reaches majority. In extreme cases, the period of limitation can span 38 years. Additionally, the doctor may also be subject to criminal prosecution for involuntary assault and battery. In that case, the patient can still submit a claim even if the medical record has been destroyed. If the patient can show reasonable grounds for the destruction of the record, the claim is not barred.

In practice, it is often difficult to ascertain how long medical documents could be useful as evidence in questions of liability. It can take years for the adverse consequences of a medical error to appear. Preserving a medical file for 30 years will suffice in many cases. Thus, modern alternatives such as destroying the file immediately after the treatment is over can be meaningful. In practice, it means that the file cannot be unambiguously ascertained. Hence, the doctor is faced with the dilemma of deciding how long the file should be preserved.

In principle, contractual obligations and other personal actions now expire after 10 years. It is possible for a doctor to make an error when treating a patient that cannot be considered a failure to fulfill his contractual obligations. In such cases, claims for compensation for damages based on the doctor's extra-contractual liability expire after five years. However, this term only starts when the patient learns of the damage and the identity of the doctor responsible for the damage. In any event, this claim expires twenty years after the treatment. If the patient was a minor when the error occurred, all these periods commence only when he/she reaches majority. In extreme cases, the period of limitation can span 38 years. Additionally, the doctor may also be subject to criminal prosecution for involuntary assault and battery. In that case, the patient can still submit a claim even if the medical record has been destroyed. If the patient can show reasonable grounds for the destruction of the record, the claim is not barred.

In principle, contractual obligations and other personal actions now expire after 10 years. It is possible for a doctor to make an error when treating a patient that cannot be considered a failure to fulfill his contractual obligations. In such cases, claims for compensation for damages based on the doctor's extra-contractual liability expire after five years. However, this term only starts when the patient learns of the damage and the identity of the doctor responsible for the damage. In any event, this claim expires twenty years after the treatment. If the patient was a minor when the error occurred, all these periods commence only when he/she reaches majority. In extreme cases, the period of limitation can span 38 years. Additionally, the doctor may also be subject to criminal prosecution for involuntary assault and battery. In that case, the patient can still submit a claim even if the medical record has been destroyed. If the patient can show reasonable grounds for the destruction of the record, the claim is not barred.
As part of the modernization of health care, the government has taken various steps toward an electronic health network. A shared patient file is accessible to all health practitioners treating the patient. The comprehensive medical file was introduced as the first step in this evolution. All the information relating to the patient's state of health is centralized in this file. The general practitioner chosen by the patient manages the comprehensive medical file. The intention of this system is to improve the quality of health care greatly by centralizing medical data so that it can be processed more efficiently, with the general practitioner as pivotal figure. This allows all those involved to follow up on the patient's state of health more efficiently. For instance, ordering the same test twice can be avoided.

The comprehensive medical file can only be used efficiently in the health care network when the information is maintained and archived in electronic form. This way everyone involved can have rapid access to the data when necessary. Nevertheless, the law still allows doctors to maintain the file in paper form instead of electronically.

The Telematics Commission was set up to avoid chaos in the electronic exchange of medical data, to ensure system interoperability and to guarantee the confidentiality and security of medical data. A telematics cell was also established within the Federal Public Service for Social Affairs, Public Health and the Environment to help achieve these goals.

The Telematics Commission developed quality criteria for computer systems used in the health care network. It also issued several recommendations relating to the preservation of medical files, specifically regarding the content of the file, the preservation period, and the form. Additionally, recommendations were issued to standardize and harmonize the content, exchange formats and syntax of electronic messages to allow a consistent integration of data in the comprehensive electronic medical file. Guidelines were formulated for the use of the electronic signature so that all persons concerned could be identified unambiguously. In this way, the origin of the information in the file can be verified and access to it restricted.
4. PROTECTING PRIVACY

Medical data are not like other data, but are highly sensitive data which are protected by the patient's right to privacy. No one would welcome having his/her medical file open to the perusal of just anyone. For this reason special care must be taken when processing medical information.

The Privacy Act and the Patients' Rights Act regulate the processing of medical data. Personal information relating to the former, present or future state of a patient's physical or mental health is medical information as defined in the Privacy Act. In principle, it is forbidden to process medical information. The only exceptions to this prohibition are those listed in the Privacy Act, for instance to create a medical file.

But there are several conditions that must be observed.

Medical information must be processed under the supervision of a health care professional. This refers to all persons who provide health care to others as part of their professional activity. This category is much broader than the category of persons that medical law obliges to maintain a medical file.

Persons processing medical information are subject to a confidentiality obligation. Most health practitioners are already subject to other confidentiality rules, for instance the professional secrecy proscribed by Article 458 of the Belgian Penal Code or the duty of confidentiality in the professional code. Article 39 of the Privacy Act also punishes breach of confidentiality as a criminal offence.

Medical information must be obtained from the person whom it concerns. This principle must prevent medical information used to provide a treatment from being collected from a variety of sources, such as other health care professionals who provided medical care.

The Patients' Rights Act reaffirms the patient's right to the protection of his privacy in each intervention by a health care professional, and in particular with regard to information relating to his state of health. This act elaborates the right of access to one's own medical information granted in the Privacy Act. The patient has the right to consult his file, with the exception of the personal notes made by the health care professional and the information relating to third parties. If desired, the patient can seek the support of a confidential counselor or request that a confidential counselor of his choice be allowed to consult the information. If this person is a health care professional, he/she will also be allowed to consult the personal notes.

Insofar as the health practitioner believes that consultation of the file would manifestly affect the patient's health in an adverse way, he can refuse to provide access to information relating to his state of health. The patient can then exercise the right of access to information relating to a health care professional's medical activity. The patient has the right to a copy of all or part of his file, under the same conditions as the right to consultation. Each copy mentions that it is strictly personal and confidential. The health care provider can refuse to give a copy if he has clear reasons to believe that the patient will use the file in a way which is contrary to public interest.

After the patient's death, the patient's spouse, civil partner, partner and blood relatives to the second degree may appoint a health practitioner to consult the deceased's file on their behalf, if their request is sufficiently motivated and specific and the patient had not expressly objected to this.

The patient has not expressly objected to this.

Digital archiving 42
Every document management system used to maintain and preserve medical files must respect the privacy of those concerned.

5. FRAGMENTED MEDICAL FILE

Every health care professional keeps a file on his/her patients and many already use electronic files. Each of these files is generally completely independent and is not co-ordinated in any way. The development of standards and the recommendation of the government is trying to lay the foundation for an electronic health network that will allow the exchange of medical information and consultation of pre-existing files by those responsible for patient care. The government is developing standards and the recommendation of the government is trying to lay the foundation for an electronic health network that will allow the exchange of medical information and consultation of pre-existing files by those responsible for patient care.

Every health care professional keeps a file on his/her patients and many already use electronic files. Each of these files is generally completely independent and is not co-ordinated in any way. The development of standards and the recommendation of the government is trying to lay the foundation for an electronic health network that will allow the exchange of medical information and consultation of pre-existing files by those responsible for patient care.
2. BASIC PRINCIPLES OF THE PRIVACY ACT

The important principles lay at the basis of the Privacy Act: legality or validity of the processing of personal data. The data controller is the one who determines the objectives of and the means used for processing personal data. If the objective and the means for processing have been established by or in execution of a law, a decree or an ordinance, the data controller is the person or entity indicated by this norm. Generally, the records creator, in other words, the person who decided to archive documents and information, is the data controller and as such he/she bears responsibility for compliance with the privacy rules.

The data controller can call upon the aid of a “processor.” A processor here means the one who actually processes the personal data at the behest and under the supervision of the data controller. This is the case when the archive is contracted out to a third party. The employees or subordinates of the data controller are not “processors” in the sense of the Privacy Act.

1.2. PERSONAL DATA

“Personal data” is any type of information relating to an identified or identifiable natural person, the data subject. A person is “identifiable” if he/she can be identified directly or indirectly, in particular by means of an identification number or of one or more specific elements characteristic of his/her physical, physiological, mental, economic, cultural or social identity.

The term “personal data” must be interpreted very broadly. It is not required that the person holding the information can identify the data subject. As soon as anyone is able to identify the person concerned using reasonable means, the information is considered personal data. For instance, an e-mail address with a pseudonym (for example incognito@provider.be) does not immediately reveal the owner of the address. The service provider probably knows who uses the address, but does not immediately reveal the owner of the address. The service provider probably knows who uses or abuses the address. The owner of the address is therefore identifiable, even if he/she does not know who uses it. This is the case when the owner of the address is not the person who processes the address. The service provider can therefore process personal data without the knowledge of the data subject.

The law applies only to a limited degree to processing carried out in whole or in part automatically and to some manual processing.

The law applies to every process that occurs in whole or in part automatically (data processing by or in execution of a law, a decree or an ordinance) and to some manual processing.

The law applies only to a limited degree to processing carried out by the security, police or intelligence services and to some manual processing. The European Centre for Missing and Sexually Exploited Children was granted a few exceptions. Additional exemptions can be granted by royal decree. These exemptions primarily impact the creation of archives, and have only a limited effect on the archive management by the archivist.

2. BASIC PRINCIPLES OF THE PRIVACY ACT

The important principles lay at the basis of the Privacy Act: legality or validity of the processing of personal data. The data controller is the one who determines the objectives of and the means used for processing personal data. If the objective and the means for processing have been established by or in execution of a law, a decree or an ordinance, the data controller is the person or entity indicated by this norm. Generally, the records creator, in other words, the person who decided to archive documents and information, is the data controller and as such he/she bears responsibility for compliance with the privacy rules. The data controller can call upon the aid of a “processor.” A processor here means the one who actually processes the personal data at the behest and under the supervision of the data controller. This is the case when the archive is contracted out to a third party. The employees or subordinates of the data controller are not “processors” in the sense of the Privacy Act.
Digital Archiving

Part 1: The Legal Framework for Business Archives

2.1. LEGALITY OR TRANSPARENCY

The legality or transparency principle signifies that anyone must reasonably be able to know what information is being processed about him or her, why this is being done and who is doing it. The data controller must provide clear information so that all those concerned are reasonably aware of which privacy expectations they may have in this respect.

In the first place, the law establishes under which conditions it is permissible to process personal data.

- The person concerned has given his/her unequivocal consent. The data controller must keep a record of this consent.
- The processing is necessary to comply with an agreement to which the data subject is a party or to take measures prior to the conclusion of this agreement.
- The processing is necessary to fulfill an obligation to which the data controller is subject by a law, a decree or an ordinance, or by an executory measure.
- The processing is necessary in pursuit of a justified interest of the data controller or of the third party to whom the data is given, except when the interests or the fundamental rights and freedoms of the person involved outweigh the data controller’s interest.

The King is authorized to exclude application of this rule in certain cases.

2.2. FINALITY

The principle of finality signifies that personal data may only be processed for a very specific, explicitly defined and justifiable purpose. Using the data for a different purpose is only permitted if this new purpose is compatible with the original one. The compatibility must be evaluated taking into account all relevant factors, specifically the reasonable expectations of the data subject, and the applicable laws and regulations.

Further processing of the data for historical, statistical or academic purposes is not considered incompatible under the conditions established by Royal Decree. The reasonableness of the data’s expiration date and the applicability of laws and regulations may be taken into account.

2.3. PROPORTIONALITY

The principle of proportionality signifies that personal data may only be processed for a very specific, explicitly defined and justifiable purpose. Using the data for a different purpose is only permitted if this new purpose is compatible with the original one. The compatibility must be evaluated taking into account all relevant factors, specifically the reasonable expectations of the data subject, and the applicable laws and regulations.

Only information that is really necessary to attain the objectives set may be processed: the data must be sufficient, relevant and may not be excessive. This does not imply that the original document must be modified. Additional remarks may be added in an annex.

Privacy data may not be stored in an identifiable way longer than necessary. The Privacy Decree contains a special regime for historical, statistical or academic purposes. When selecting documents for the archives, the proportionality principle will have an important role to play.

The legality of transparency principles signifies that anyone must reasonably be able to know what information is being processed about him or her. This does not imply that the original document must be modified. Additional remarks may be added in an annex.

Integrating the practical effects of these principles with the legal framework for business archives is an important task. The following principles are important for the private sector.

2.1. LEGALITY OR TRANSPARENCY

2.2. FINALITY

2.3. PROPORTIONALITY

The King is authorized to exclude application of this rule in certain cases.
3. DATA SUBJECT PROTECTION RIGHTS

3.1. NOTIFICATION RIGHT

The data controller must, in principle, notify all data subjects that information about them is being processed. The law makes a distinction depending on whether the information came from the data subject himself or from another source.

3.1.1. Data Received from Data Subject

An organization will mainly archive personal data requested directly from the data subject. Examples of this are the personnel files or customer information. In principle, the data subject must be notified about the objective and the context of the processing at the latest upon the time of collection, except if he is already aware of this information. Additional obligations can be proscribed for specific situations by royal decree. The notification should specifically contain the following information:

- the name and address of the data controller and, where appropriate, his representative
- the purposes of the processing
- the recipients or the categories of recipients of the data
- information on whether an answer is mandatory and the possible consequences of not providing an answer
- a notice that the data subject has the right to consult and correct his/her own personal data.

Personal data may only be preserved for as long as they are required in order to achieve the purposes for which they were collected. When archiving is a goal in itself, the organization should state this when collecting the information.

3.1.2. Data Received from Another Source

When the data has not been received from data subject, there is no immediate occasion to provide the required notification. The law gives data controller several options: he/she contacts the data subject immediately after receiving the information or he/she notifies the data controller. Additional obligations may be proscribed for specific situations by royal decree.

The notification must contain the following information:

- the name and address of the data controller and, where appropriate, his representative
- the purposes of the processing
- notice that the data subject has the right, upon request and at no cost, to oppose the processing of his personal data for the purpose of direct marketing. In this case, the person must be informed before the personal data are given to a third party. The person must be informed before the personal data are given to a third party. The person must be informed before the personal data are given to a third party. The person must be informed before the personal data are given to a third party.
- the categories of data involved
- the recipients or categories of recipients

An organization will mainly archive personal data requested directly from the data subject.

3.1. NOTIFICATION RIGHT

The data controller must, in principle, notify all data subjects that information about them is being processed. The law makes a distinction depending on whether the information came from the data subject himself or from another source.
There are only a few exceptions to the communication right. Anyone concerned has the right to be informed when the information is disclosed.

3.2. COMMUNICATION RIGHT

The Privacy Act gives everyone the right to determine how his personal data are processed. In order to exercise this right, the data controller must send a dated and signed request to the data controller, his representative in Belgium or the processor. The request must include the name, address and the reason for the request. The data controller must respond within one month of receiving the request.

If the processing is performed by the government bodies listed in the law, there are no special requirements. However, the data controller must notify the person concerned if the data is processed by another country.

47
3.3. CORRECTION RIGHT

Everyone has the right to have all incorrect personal data relating to him/her corrected at no cost. In addition to correcting inaccurate data, the person concerned may also provide supplementary information. When information is processed in contravention of the law, he/she may demand that it be deleted, or at least no longer used.

The data subject may not simply replace subjective evaluations with his/her own version, but the data controller must record that the information is challenged.

In other cases, too, it can be advisable not to make changes and additions to the original document but to place them in an annex.

The Privacy Act gives the data subject two special remedies against violations of this right.

3.5. RIGHT TO REDRESS

The procedure for invoking the right to object is the same as for the correction of incorrect data.

There are only a few exceptions to the right to make corrections, again for those government bodies listed in the law. In this case, too, the right to make corrections must sometimes be exercised through the Commission for the Protection of Privacy.

The Privacy Act gives the data subject two special remedies against violations of this right.

3.4. RIGHT TO OBJECT

Every data subject may object to the processing of his/her personal data if he/she has weighty and justified reasons for doing so. One may object to processing for direct marketing purposes without any specific motivation.

The right to object does not apply when the processing is necessary:

- to fulfill an obligation prescribed by law or to which data controller is subject;
- to execute an agreement to which the person concerned is a party or in which he agrees in accordance with which the person concerned is a party or in which he agrees;
- to ensure the performance of contract.

The rights of data subjects can be exercised without any specific motivation. When collecting data, the data controller must give the data subject an opportunity to object to the use of his/her details for direct marketing.

The procedure for invoking the right to object is the same as for the correction right. The data controller must notify the requestor within a month about what action he will take.

In addition to those already mentioned, there are a few other exceptions for some public bodies.
The processing is necessary when the data subject has explicitly...

**4.1. SENSITIVE DATA**

Personal data revealing the fact of having an opinion in political, religious or philosophical convictions or union membership, and personal data regarding sexual orientation all fall under the category "sensitive information." Sensitive information may be processed in the following cases:

- The data subject has given written permission for such processing, on the condition that he/she may withdraw this permission at any time. This exception cannot be invoked by present or potential employers of the data subject, or by any person with whom the data subject is in a position of dependence.
- The processing is necessary for the realization of an operative establishment
- The processing is necessary to allow the data controller to comply with specific obligations and rights arising from labor law;
- The processing is necessary to allow the data controller to comply with the order of the national labor inspection.
- The data subject has given written permission for such processing of such sensitive information.
- The processing is necessary in the context of medical research, insofar as the conditions established in the Royal Decree are met.
- The processing is necessary for the academic research, insofar as the conditions of the right in court.
- The processing is necessary for the establishment's exercise of defenses or a made public;
- The processing relates to information that the data subject has indisputably...

4. PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

In addition to the rules already discussed, there is a more stringent regime for certain categories of personal data.
4.2. MEDICAL INFORMATION

This category covers all information related to health. The law does not explain this term further, but it refers to “all personal information relating to the former, present or future state of a person’s physical or mental health.”

Medical information may be processed in the following cases:

• The data subject has given written permission for such processing, on the condition that he/she may withdraw this permission at any time. This exception cannot be invoked by present or potential employers of the data subject, or by any person with whom he/she is in a position of dependence, unless the object of the processing is to provide a benefit.

• The processing is necessary to allow the data controller to comply with specific obligations and rights relating to labor law;

• The processing is necessary to reach an objective established by or by virtue of the laws governing social security.

• The processing is necessary to reach an objective established by or by virtue of the law governing health care professionals and medical disciplines, or to comply with specific obligations, and rules governing the exercise of the profession of medical practitioner.

• The processing involves information that the person concerned has indisputably made public.

• The processing is necessary to establish, exercise or defend a right in court.

• The processing involves information that the person concerned has already made public for academic research.

• The processing involves information that the person concerned has already made public for academic research for academic research.

• The processing involves information that the person concerned has already made public for academic research.

• The processing involves information that the person concerned has already made public for academic research.

Beyond these specific cases, medical information may be processed in all cases in which this is required by a law, decree, ordinance, or a ministerial order for reasons of grave public interest. All processing must be done under the supervision of a health care professional bound by secrecy. Moreover, medical information may be used for academic research only when the conditions established in the Royal Decree are met.

The data subject also has a right to have his medical information communicated to him/her. Both he and the data controller can request that the information be consulted through the mediation of a doctor or other professional health care provider.

4.3. JUDICIAL INFORMATION

Personal data relating to disputes submitted to tribunals and courts as well as to administrative tribunals, relating to accusations, prosecutions or judgments dealing with criminal offenses or relating to administrative penalties or security measures are all considered judicial information.

The following are among the exceptional cases when judicial information may be processed:

• The processing is necessary for the management of the data subject’s own disputes or those of the data controller.

• The processing is necessary for academic research, insofar as the conditions established in the Royal Decree are met.
Judicial information may be processed if this is necessary to achieve the objectives that a law, decree or ordinance, a royal decree or a ministerial order has established\textsuperscript{167}. In cases where the data controller is allowed to process judicial information, he is bound by an obligation of secrecy.

4.4. ARCHIVING SENSITIVE, MEDICAL AND JUDICIAL INFORMATION

The initial gathering and processing of these special categories of information must fall within the scope of one of the exceptions listed in the Privacy Act and must satisfy the numerous conditions that are set. The preservation of this information must also be justifiable on the same or another legal basis.

Communicating special personal data is, in itself, a type of processing and is only possible when the legal basis invoked justifies this. To the extent that archiving takes place internally (by subordinates or by a processor) this is not an issue, as there is no communication to third parties going on. All employees must be bound by an obligation of confidentiality.

Granting access to the archives is an entirely different situation. There must be a legal basis for the communication of the data. The Privacy Act permits communication in relation to a legal dispute one is involved in or for academic research, albeit under the conditions established by Royal Decree\textsuperscript{168}.

In order to be able to comply with the stipulations of the Privacy Act efficiently, the metadata of documents and files in the archive should mention whether they contain sensitive, medical or judicial information.

5. ADMINISTRATIVE PROVISIONS

5.1. REGISTRATION

The data controller must register his activities with the Commission for the Protection of Privacy before he starts processing personal information\textsuperscript{169}. There are many exceptions to this rule, in order to limit the amount of registrations\textsuperscript{170}. Among the exemptions are processing as part of salary administration, personnel administration, accounting, customer and supplier relationship management, municipal registers and processing by government administrations\textsuperscript{171}. The Privacy Decree imposes special conditions in each case.

5.2. AUTHORISATION BY THE COMPETENT SECTORAL COMMITTEE

As of 2003, the law allows sectoral committees to be established within the commission. These sectoral committees are competent to examine and decide upon all requests relating to the processing or communication of information governed by any special legislation\textsuperscript{172}. An existing example is the sectoral committee for social security\textsuperscript{173} and the sectoral committee for the federal government established by the Privacy Act\textsuperscript{174}. In principle, any time the federal government wishes to communicate personal data, authorization is required from the federal sectoral committee, which investigates whether the communication complies with the laws and rules\textsuperscript{173}. 
6. MISCELLANEOUS PROVISIONS

The Privacy Act regulates various other aspects of the processing of personal data. A short overview is given here for the sake of completeness. Only aspects that are of specific importance for digital archiving are elaborated further.

6.1. SECURITY AND CONFIDENTIALITY OF DATA PROCESSING

The data controller must take suitable technical and organizational measures to protect personal data against fortuitous or wrongful destruction, accidental loss, modification, unlawful access and any unlawful processing in general. An appropriate level of security must be guaranteed given the state of the art in technology, the costs involved, the nature of the data to be protected and the potential risks. In other words, the data controller must ensure the confidentiality and integrity of the information contained in the data.

The Privacy Act lists several specific objectives that the data controller must satisfy. A procedure should be in place for updating information so that incorrect, incomplete, irrelevant and unlawfully obtained or processed information can be corrected or removed. Access to the data and processing tools may only be entrusted to employees and other subordinates to the extent necessary for the execution of their responsibilities and the operational needs of the organization. The employees concerned must be educated about the applicable privacy regulations. The actual processing of information must correspond to the activities mentioned in the registration to the Privacy Commission.

If the data controller outsources certain tasks, he must choose a processor that guarantees a sufficient level of security. The outsourcing contract must describe the technical and organizational security measures, as well as the liability of the processor for damages resulting from non-compliance. The processor must certify that the processing is carried out in accordance with the conditions laid down in the contract, and must be subject to the same privacy obligations as those to which the data controller is bound. The contract must be drafted in writing, on paper or in electronic form.

6.2. CROSS-BORDER DATA EXCHANGE

The law regulates the transmission of data to third countries more stringently than the exchange of data among EU countries. In many countries, a much lower standard of protection for personal data is in place.

The question whether the level of protection is sufficient in a certain country can be answered in general. Each case must be examined individually, taking into account the nature of the data, the objectives and the duration of the intended processing, the countries of origin and destination, the general and sectoral legislation in these countries, as well as the professional codes and protective measures observed in the countries.

Under certain circumstances, data may still be exchanged with countries that have a much lower standard of protection for personal data. This is the case when all those involved have given their unequivocal permission or when the information is used in preparation of or in the execution of a contract with the data subject. This is also allowed in order to defend a right in a legal dispute or when the interest of the data subject is at stake.
7. CASE STUDY: ARCHIVING PROFESSIONAL E-MAIL

When the need for protection do not belong to the person convicted, 

7.1. FREEDOM OF COMMUNICATION

when the need for protection do not belong to the person convicted, 

6.3. PENALTY PROVISIONS

After authorization from the King, the personal data may then be transmitted. 

The data controller himself can guarantee sufficient protection, for instance by 

including privacy protection obligations in the contract with the foreign recipient. 

After authorization from the King, the personal data may then be transmitted. 

Monitoring some electronic communications even without accessing the content.

...
The confidentiality of telecommunication entails that an employee's e-mail may not be added to the company archive just like that. An absolute prohibition on accessing an employee's mailbox is untenable in a professional context. On the one hand the employer feels the need to supervise the use that his employees make of e-mail. On the other hand, important business information must be accessible to the company. For instance, communication via e-mail is increasingly being used as evidence in court.

Confidentiality of telecommunication is not an absolute right. In cases where all the participants to a communication give permission for the interference, no offence is committed. In addition, there is an exception for cases where a law permits or requires the interference. This exception is primarily intended to allow wiretapping as part of a criminal inquiry, as circumscribed in the Wiretap Regulation. Some legal scholars see another example in the relationship of subordination between the employee and his/her employer. On this basis, the employer may monitor the employee's use of internet and e-mail, and may also set up an archive containing professional messages. Nonetheless, the Privacy Act still applies and determines the limits the employer must respect when exercising this supervision.

7.2. COLLECTIVE LABOR AGREEMENT (CLA) NO 81 ON THE PROTECTION OF PRIVACY IN THE MONITORING OF ELECTRONIC ONLINE COMMUNICATION DATA

Thus far, the monitoring of abuse of e-mail and internet facilities at work has received more attention than the issue of archiving. Concerns about monitoring both on the part of employers as of employees led to the negotiation of CLA no 81. The employers' organizations and the trade unions looked at all the applicable legislation and applied these to work environment in a way that balances the interests at stake. Although this was not the CLA's primary intention, the agreement does have an impact on archiving professional e-mail in the private sector.

The CLA elaborates the three basic principles from the Privacy Act: transparency, finality and proportionality. The employer must take these principles into account when he sets up an archiving system as well as during its use.

In a first phase, the employee must devise an adequate archival policy which specifies how the monitoring will be carried out. The archiving policy must be explained to the employees. The employee must also devise a monitoring procedure which involves setting up a detailed archival policy, which establishes the categories of e-mail messages to be saved as well as the metadata to be added to each message. The archiving policy should explain to the employees which type of personal data will be kept in the archives and how this type of data will be archived. The policy should explain the objectives pursued, the place and duration of preservation of personal data, whether or not monitoring is permanent or happens sporadically, and whether any penalties will be imposed.

By virtue of the proportionality principle, only professional e-mail may be pre-accessed.
is considered private except when the employee "does not cast doubt" upon its professional nature. This description is extremely vague and difficult to apply in practice. The employer would do well to ask his employees to indicate explicitly for each outgoing and incoming message whether or not it is professional.

According to the CLA, professional e-mail may be archived without further ado for future use within the company. Private e-mail may only be consulted in a limited number of cases, for instance in order to monitor abuse.

The monitoring of the use made by employees of e-mail and internet must be executed in two distinct phases: the same applies to monitoring of compliance with the archival policy. In the first phase, the monitoring should be done at a general level and only anonymous data should be processed. If this brings to light evidence of non-compliance with the archival policy, the employer should explain the policy again to his personnel and warn them that if a similar violation occurs in the future, those responsible will be identified. This procedure shows that the CLA is primarily aimed at restraining abuse and not at supporting normal business processes, such as archiving professional information. Assessing the archival value of e-mail anonymously is extremely difficult. Organizations should put at least as much effort into encouraging employees to archive information as in monitoring their behavior.

The CLA only covers the relationship between the employer and his employees, without giving any regard to the position of third parties, for instance business contacts. In any case, the rules of the Privacy Act also must be respected with regard to those persons mentioned in the outgoing messages. Correspondents must be informed about the processing of their data. This can be done by including a notice to this effect at the bottom of each outgoing e-mail message. An automatic response with this information could also be sent to new correspondents contacting the organization spontaneously.

Every organization must set up its information systems taking into account the requirements of the Privacy Act. Likewise, it should ensure that its documents, for instance business contacts, are not copied without the consent of the relevant third parties. This can be achieved by adding certain metadata to its documents, for instance, a list of data subjects, the nature of the information, which notification was made, …

Implementing privacy regulation in practice is a complex matter. It is essential to draft a well-considered privacy policy. Processing e-mail in contravention of the law can have grave consequences, as the data involved must, in principle, be destroyed.
1. INTRODUCTION

2. SCOPE OF APPLICATION

2.1. ORIGINALITY

2.2. FORM

COPYRIGHT LAW PROTECTS TEXTS, IMAGES, MUSICAL COMPOSITIONS, COMPUTER PROGRAMS, AND ANY OTHER WORKS AS LONG AS THEY POSSESS A MINIMAL DEGREE OF ORIGINALITY AND EXPRESS THE PERSONALITY OF THE CREATOR.
3. THE COPYRIGHT HOLDER

Copyright is a personal right. The copyright holder is the person who created the work or, in the case of a work created by several people, the person(s) who contributed most to the creation of the work. The copyright holder has the exclusive right to reproduce, distribute, display, and perform the work in public. These rights are transferable by contract or through遗嘱.

In the context of business archives, the person who created the work is often the initial copyright holder. In cases where the work is created by multiple authors, the copyright may be jointly held or divided among the contributors.

4. PROPERTY RIGHTS

The copyright holder has the exclusive right to reproduce, distribute, display, and perform the work in public. These rights are transferable by contract or through遗嘱. In the context of business archives, the person who created the work is often the initial copyright holder. In cases where the work is created by multiple authors, the copyright may be jointly held or divided among the contributors.

4.1. PROPERTY RIGHTS

The copyright holder has the exclusive right to reproduce, distribute, display, and perform the work in public. These rights are transferable by contract or through遗嘱. In the context of business archives, the person who created the work is often the initial copyright holder. In cases where the work is created by multiple authors, the copyright may be jointly held or divided among the contributors.
Copyright law has an impact on digital archiving in various ways. The archivist or records manager must copy the work to include it in his/her archive. Over time, the work must be adapted so that it remains accessible for the future. Finally, it is also the intention to make the work available to others, either the general public or a select group.

4.2. MORAL RIGHTS

The initial author has the right of disclosure or disclosure: only he/she may decide when the work is ready to be made public. The paternity right implies that the author decides under what name the work will be published. The author can oppose any modification to this primary version. He/she can also decide under what name the work will be published. The author can oppose any modification to this primary version.

Moral rights are personal, which means they are linked to a particular person and are not transferable. The moral rights protect the "intimate bond" between the author and his/her creation, which is considered an expression of his/her personality. An organization can never be the holder of the moral right of a work since this is not transferable.

4.3. EXCEPTIONS TO COPYRIGHT

From the very beginning when copyright was first introduced in 1886, the legislation included certain exceptions. These exceptions are also called "compulsory licenses" or "legal licenses." Broadly speaking, the exceptions apply to the private use of works in education, broadcasting on radio or television, performance in public, and the like. These exceptions are also called "compulsory licenses" or "legal licenses."
6. TERM OF PROTECTION

The original author is not required to exploit his work himself. He may authorize others to do so. The agreement whereby an author grants permission to a third party to exploit his work or in which ownership of copyrights are transferred, is called a “license agreement”.

The Copyright Act imposes several special conditions upon license agreements to protect the author. Only a written license agreement has evidential value against the author. The license must expressly state if and how the author will be remunerated, as well as the extent and duration of the transfer of rights per mode of exploitation. The transfer of the rights for modes of exploitation still unknown is null and void. The licencee is obliged to actually exploit the work in good faith and in accord with the permission. The licencee must expressly state if and how the author will be remunerated.

There are more flexible arrangements for works created as part of an employment contract or an appointment of a civil servant. The relaxation applies exclusively for works created in the execution of the employment contract or appointment. Moreover, the employment contract or appointment must expressly provide for the transfer of copyrights. Insofar as these conditions are fulfilled, the transfer may relate only to the employment contract or appointment in which the work is created, but not to other employment contracts or appointments. The transfer of copyrights runs until 70 years after the death of the longest surviving author. Copyright protection runs until 70 years after the death of the author. If more than one person is the author, the copyright protection runs until 70 years after the death of the last surviving author.
In the case of the employee's work, the copyright holder has the right to determine the conditions of the work. This right is also known as the moral rights of the author. The work can be used in a manner that is designed to exploit the work's expressive and physical qualities. In the case of the employee, the conditions of use are negotiated with the employee. The employee is not allowed to reproduce or distribute the work without the permission of the copyright holder.

The Copyright Act imposes specific sanctions on copyright infringement. The act gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to reproduce. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to distribute. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to perform. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to display. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to make derivatives. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to perform.

The conditions of use are negotiated with the employee. The employee is not allowed to reproduce or distribute the work without the permission of the copyright holder. In the case of the employee, the conditions of use are negotiated with the employee. The employee is not allowed to reproduce or distribute the work without the permission of the copyright holder.

The Copyright Act imposes specific sanctions on copyright infringement. The act gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to reproduce. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to distribute. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to perform. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to display. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to make derivatives. The act also gives the author the right to exclude the use of the work by others. This right is known as the exclusive right to perform.

The conditions of use are negotiated with the employee. The employee is not allowed to reproduce or distribute the work without the permission of the copyright holder. In the case of the employee, the conditions of use are negotiated with the employee. The employee is not allowed to reproduce or distribute the work without the permission of the copyright holder.
9. SPECIAL PROTECTION FOR COMPUTER PROGRAMS

9.1. DEFINITION OF THE TERM "COMPUTER PROGRAM"

No definition of the term "computer program" is provided in the law. The English translation of the term "computer program" will be discussed in what follows.

Copyright protection for computer programs is regulated in the law of 30 June 1994 on the legal protection of computer programs. A few particularities of this law Copyright protection for computer programs is regulated in the law of 30 June 1994 on the legal protection of computer programs. A few particularities of this law.

9.2. CIVIL SANCTIONS

The copyright owner can enter a claim for damages for copyright infringement based on the general liability rules in the Belgian Code of Civil Law. To do this, three things must be proven: wrongful act, harm and the causal connection between the two. Breach of the copyright provisions is always a wrongful act. Malicious intent or fraudulent purpose is not required: even someone who infringes a copyright in good faith can still be held liable. The harm can take various forms, including lost profit and moral harm which will be cited frequently. Judges often measure harm based on the rates used by copyright collecting societies or those customary in the relevant industry. Case law recognizes the causal relationship between the copyright infringement and the harm suffered fairly easily, especially in a commercial context.

In exceptional cases, the nature of the copyright infringement is such that awarding even a minimal amount of damages is disproportionate. Sometimes bringing suit is an exaggerated measure. In such cases, the person who is strictly speaking committing a copyright infringement can counterclaim that the author is abusing the rights granted by copyright law. This could also be the case where the infringer has destroyed the evidence of infringement by the author. The Judicial Code contains several special procedures to help the author defend his rights. The Copyright Act provides the author with two ways to protect his rights: seizing forgeries and entering a petition for injunctive relief.

The Judicial Code contains several special procedures to help an author defend his rights. The Copyright Act provides the author with two ways to protect his rights: seizing forgeries and entering a petition for injunctive relief.

8.2. CIVIL SANCTIONS

Copyright protection for computer programs is regulated in the law of 30 June 1994 on the legal protection of computer programs. A few particularities of this law. Copyright protection for computer programs is regulated in the law of 30 June 1994 on the legal protection of computer programs. A few particularities of this law.
expressed in any form, language, notation or code, the purpose of which is to cause a computer to execute a particular task or function. Thus on the one hand computer programs are a kind of text, and on the other hand it encompasses a set of instructions.

In practice these copies exist in the copy that the computer reads into the work.

9.2. THE COPYRIGHT HOLDER

For computer programs too, the initial author is the person who created the program. This rule is however mitigated in favor of employers. Only the employer is considered to be the holder of the property rights to a computer program written by one or more employees or civil servants in the execution of their tasks or at the request of the employer, unless the contract or appointment states otherwise.

9.3. EXTENT OF THE PROTECTION

A computer program is protected by the same property rights as any other work, but the moral rights are more limited. The author of a computer program has no right of divulgation, but does have the right to be credited with the authorship and the right to forbid any modification of his/her work to the extent that this would damage his/her honor or his/her reputation.

9.4. COPYRIGHT EXCEPTIONS

The author's exclusive rights are so extensive that normal use of his programs is forbidden, unless the author gives his express consent. Of course, this is not the intention of the copyright law. In order to strike a just balance, several specific exceptions have been introduced in favor of the legitimate user. This is any person who is in possession of a legally obtained copy of the program.

First and foremost, the legitimate user may use the program for the purpose for which it was created. The user may make copies, modifications and may correct any errors that may be present without the author's permission.

In practice, these copies refer to the copies that the computer loads into the working memory when it runs a program. The users' agreement may impose restrictive conditions, but, of course, it cannot forbid the loading and running of the program. The contract may not forbid the correction of errors, since such errors can hinder normal use.

And the legitimate user may make one single backup copy of the program. He may not pass this backup on to another user, because it is necessary to work with his/her copy of the program.

The above exceptions are so extensive that normal use of this programs is protected by the same property rights as any other work.

4. COPYRIGHT EXCEPTIONS

This concept of this Regulation.

9.3. EXTENT OF THE PROTECTION

For computer programs too, the initial author is the person who created the program. This rule is however mitigated in favor of employers. Only the employer is considered to be the holder of the property rights to a computer program written by one or more employees or civil servants in the execution of their tasks or at the request of the employer, unless the contract or appointment states otherwise.

9.2. THE COPYRIGHT HOLDER

A computer program is protected by the same property rights as any other work,

The user is therefore unable to evade the copyright and will have consider each program as potentially covered by copyright.

The use of identical material is easier to achieve the originality and will have consider each program as potentially covered by copyright.

The user is therefore unable to evade the copyright and will have consider each program as potentially covered by copyright.
a search system. A database can exist in paper or electronic form.

When collection each time is done by adding the elements or setting up a random collection of elements. It is not a database if the collection is not systematic or methodical ordering. The order by systematic arrangement of a larger whole, such as in a book, magazine or periodical, does not suffice. A database is a collection of independent works. Databases are protected in two different ways: the database as a whole and each of its element.

10. SPECIAL PROTECTION FOR DATABASES

A "database" is a collection of independent works. Databases are protected in two different ways: the database as a whole and each of its elements.

10.1. DEFINITION OF THE TERM "DATABASE"

A database is a collection of independent works. A database can exist in paper or electronic form. Including a computer program in the archive does not constitute this criminal offence. Making a computer program available to others outside the workplace, if it is used by employees and third parties, could be construed as illegal trade.

When collection each time is done by adding the elements or setting up a random collection of elements. It is not a database if the collection is not systematic or methodical ordering. The order by systematic arrangement of a larger whole, such as in a book, magazine or periodical, does not suffice. A database is a collection of independent works. Databases are protected in two different ways: the database as a whole and each of its elements.

9.5. PENAL SANCTIONS

There is an additional offence relating to computer programs: putting a copy of a computer program on the market or possessing a copy for commercial reasons whilst one knows or could reasonably know that the copy is illegitimate. This provision is broader than the offences described in the Copyright Act. A copy of a computer program can be a material copy (CD-ROM) or an immaterial copy (on a website). In addition to commercializing illegal copies, distributing them without a commercial objective is also punishable. This also covers free, online distribution of a copy. Reasonably knowing is a considerably weaker condition than knowingly and willingly. The penalty is a fine between 100 and 100,000 EUR, multiplied by a factor of five.

including a computer program in the archive does not constitute this criminal offence. Making a computer program available to, or allowing it to be consulted by, employees and third parties constitutes this criminal offence.

When collection each time is done by adding the elements or setting up a random collection of elements. It is not a database if the collection is not systematic or methodical ordering. The order by systematic arrangement of a larger whole, such as in a book, magazine or periodical, does not suffice. A database is a collection of independent works. Databases are protected in two different ways: the database as a whole and each of its elements.

A database is a collection of independent works.


The sui generis database right sets other criteria than copyright law to determine who holds the copyright and the sui generis database right.

10.2. HOLDER OF THE COPYRIGHT AND THE SUI GENERIS DATABASE RIGHT

The general copyright rule also applies to databases: the author is the one who created the database. For one category of databases the law presupposes that only the employer is the owner of the economic rights. This is the case when the database was developed by one or more employees or civil servants when performing their duties or following instructions from their employer, as long as the database does not belong to the cultural sector or the employer's contract or the civil servant's appointment does not state otherwise. Collective labor agreements can stipulate further details. The law does not define the term "cultural sector," which means that the courts will have to interpret this concept.

The sui generis database right does not protect the intimate bond between an author and his creation, but does protect the investment made by the producer of the database. Only producers established in an EU Member State enjoy the right to this protection. Producers from other countries can obtain the same protection when there is an agreement on this matter between the EU and the country in question. Such agreements can only be entered into if the law of the member state of the database producer sets other criteria than copyright law to determine who holds the sui generis database right.

10.3. EXTENT OF THE COPYRIGHT PROTECTION

The special regime for databases applies to the database as a whole and does not cover the elements included in it. The "database as a whole" means the database's structure and presentation. The special regime applies to the database as a whole and the database's selection or ordering of its contents can demonstrate its originality. However, the value of many databases lies in their completeness and functionality, two characteristics that often exclude originality. For instance, the phone book is always ordered alphabetically. The selection or ordering of the database's contents can thus have been satisfied. The question of obtaining or ordering the database's contents can be left to the discretion of the database producer. The special regime for databases applies to the database as a whole and does not overlap with countries offering comparable protection. Thus far, few countries have such laws.

10.4. EXTENT OF THE SUI GENERIS DATABASE RIGHT

The sui generis database right applies when the obtaining, verification or presentation of the contents required a substantial investment in a qualitative or quantitative sense. The required investment can be a monetary investment or an investment of time or effort. Only a substantial investment is taken into account. "Substantial" can refer to a large quantitative investment or an important qualitative investment. The producer must be able to demonstrate that these conditions have been fulfilled.
The objective of the sui generis database right is to protect the producer's investment by granting him an exclusive right to the exploitation of the database. More specifically, the producer may impose restrictions on the retrieval and reuse of the database: "Extraction" is permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form.218 "Re-utilization" is any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission.219

The producer can forbid the extraction or re-utilization of the database as a whole or of a substantial part of it. The criterion "substantial part" must be evaluated relatively and is proportionate to the damage done to the producer's investment. A part can be substantial because of the amount of information (quantitative criterion) or because of the nature of the data (qualitative criterion) that is extracted or re-utilized. In some cases, the producer may also forbid the extraction or re-utilization of a non-substantial part, namely when this conflicts with the normal exploitation of the database or when this would unreasonably prejudice the legitimate interests of the producer.220

The records manager will frequently have to archive complete databases. In that case, there is a question of extracting the database as a whole. In principle, the producer must give his/her permission for this. Making the database available to the public can then be a type of re-utilization.

10.5. SANCTIONS

A violation of the copyright on a database is punishable in accordance with the general rules of the Copyright Act. The Belgian Database Protection Act creates several sanctions to protect the sui generis database right, which run parallel to the sanctions in the Copyright Act. Three types of actions are considered forgery: the malicious or fraudulent violation of the producer's rights, the malicious or fraudulent use of the producer's name or of a distinctive characteristic with which he signs his property (e.g., a logo), and finally the misuse of databases. The judge can also order the publication of the verdict and the closure of the perpetrator's establishment.221

The penalty is identical to that set by copyright law. The judge can also order the restoration of the databases. The perpetrator knows that the databases have been created.

The records manager must keep a record of the databases that are extracted or re-utilized.

The database is not protected against the unauthorized extraction or re-utilization of databases that are freely available to the public. Making the database available to the public may also constitute a violation of the producer's rights. The author or licensee may object to the use of the database if the use conflicts with the normal exploitation of the database or if it would unreasonably prejudice the legitimate interests of the producer.222

The consequences of a database right are similar to those of a copyright. By taking a copier or other means of extraction or re-utilization of the database, the producer may obtain an exclusive right to the exploitation of the database. The producer may also impose restrictions on the retrieval and reuse of the database. The producer may also impose restrictions on the retrieval and reuse of the database.

11. CASE STUDY: ARCHIVING THE COMPANY WEBSITE

Whereas copyright has little impact on a company's paper archive, it must be given due consideration when establishing a digital archive. The inclusion of a document in the archive requires the creation of various copies. Moreover, these copies must be made permanent. Granting employees access to the archive is a type of communication to the public, even though this may be an extremely limited public. All these actions fall under the copyright holder's monopoly.

Copyright, in a broader sense, also includes the right to communicate to the public other than by means of a public performance. The right to communicate to the public other than by means of a public performance includes the right to make available to the public a substantially author's database.

The purpose of archiving is to protect the databases that are created by the company.
The impact of copyright law on the digital archive and the options open to the archivist are explained below by way of a practical example, more specifically archiving a company website. Organizations may wish to archive their websites for evidence purposes, for instance, in order to demonstrate compliance with disclosure requirements imposed by law.

11.1. CREATING A CORPORATE WEBSITE

In general, a website is not created by one person, but by a whole team. A graphics designer designs a logo and the style for the website. A web developer transforms this design into a usable template. A photographer provides pictures. All these elements together create a site's look and feel, which can be protected by copyright.

The content of a corporate website, such as product documentation, reports or annual accounts, is protected by copyright. The respective authors of these texts are the original holders of the copyright.

11.2. ARCHIVING THE COMPANY WEBSITE

There are various strategies for archiving websites. One possible option is to make a copy of all the files used to construct the site. Often certain changes must be made to preserve the site and keep it accessible.

For dynamic websites driven by databases, this may be too complicated or too expensive. In this case, a screen capture movie can be made showing how visitors view the site.

In both cases, a copy of the site is produced for archival purposes. The screen capture can even be seen as a derivative work, which may be protected by copyright.

For dynamic websites, a specific archival license agreement with all involved copyright holders is necessary in order to archive the site. In this case, a screen capture movie can be made showing how visitors view the site.

11.3. ARCHIVAL LICENSE

While archives and libraries in the public sector can invoke certain copyright exceptions, this is not the case in the private sector. Companies must obtain the necessary licenses to construct and use their archive. A specific archival license or a general transfer of copyrights are two possible avenues.

11.3.1. ARCHIVAL LICENSE

The company can opt to enter into a specific archival license agreement with all involved copyright holders. This license agreement needs to be negotiated with all involved parties.

The company can enter into a specific archival license agreement with all involved copyright holders. This license agreement needs to be negotiated with all involved parties.

The company can enter into a specific archival license agreement with all involved copyright holders. This license agreement needs to be negotiated with all involved parties.

The company can enter into a specific archival license agreement with all involved copyright holders. This license agreement needs to be negotiated with all involved parties.

In general, a website is not created by one person, but by a whole team. A graphics designer designs a logo and the style for the website. A web developer transforms this design into a usable template. A photographer provides pictures. All these elements together create a site's look and feel, which can be protected by copyright.
Part 1: The Legal Framework for Business Archives

The position line remains the same as the output. The introduction of the electronic signature is a fundamental change in the context of digital document management. The General Public License (GPL) and the Lesser General Public License (LGPL) are common examples for computer programs.

A third possibility consists in requesting the respective authors to release their work under a standard open source license. The various Creative Commons Public Licenses are often used for texts, music, and images. One characteristic of these licenses is that the author grants non-exclusive and generally transferable rights to copy, distribute, and create derived works. The conditions for each mode of exploitation must be specified in the respective licenses.

Archiving is Copying

Copyright law provides an exception for archiving protected works. In most cases, the only way to archive a work is to make a copy while preserving the original work. However, the law also allows for the archiving of works that have been made by the employee in the course of his or her work.

As early as possible, organizations and employers should negotiate consent for archiving. This consent should cover existing and future modes of exploitation and must be specified in detail.

In the text, the concept of archiving is described as copying. The archiving of works that have been made by the employee in the course of his or her work is considered copying. The law does not protect the employer's interests in these cases. However, the employer can still claim the right to use the work in the course of the employee's work.

In conclusion, the legal framework for business archives is complex and requires careful consideration of the rights and interests of all parties involved.
Various techniques can be used to produce an electronic signature. The most

THE DIGITAL SIGNATURE TECHNOLOGY

L. ANNEX 1.
Hashing is a technique with which electronic information can be reduced to a unique fixed-length code. By applying various mathematical functions to the document, the hashing algorithm calculates a hashing code. This hashing code is unique for each document and is why it is also called a digital fingerprint. If even a single character in the digital document is modified in transmission or storage, the resulting hashing code will be different. By comparing the original hashing code with the current one, one can determine whether a document has changed or not.

A simple example can illustrate this. A simple hashing algorithm could work as follows: replace each letter in the text of the message with its position in the alphabet, add all these numbers together, and if the sum reaches one million, replace each letter by its position in the alphabet again. The end result will be a number smaller than one million. That number is the hashing code. If even one letter in the text of the message changes, the hashing code will be different.

The original fingerprint must be safeguarded against manipulation to allow the original hashing code to be compared with the present hashing code. Encryption techniques are used to achieve this.

 hash code Hashing algorithm Electronic document
Encryption or cryptography is the science that investigates how information can be safeguarded from, among other things, unauthorized access. In antiquity, Julius Caesar used simple encryption algorithms to exchange messages with his generals. Encryption or encoding means that the original plaintext message is transformed into a cipher text that appears meaningless. The reverse operation is called decryption or deciphering. A key known only to the sender and recipient can be used for encrypting and decrypting. Encrypting the content of a message prevents others than the sender and recipient from being able to read it. In addition, it is certain that an encrypted message that can be deciphered by using the common secret key originated from one of these two parties. This ensures the confidentiality of the message.

However, there are many disadvantages to symmetric cryptography. The two parties, who need a secret key for each message, must exchange the key beforehand. This can be done using a secure channel, but this is not always possible or practical. In addition, symmetric cryptography is vulnerable to key compromise, as any party with the secret key can decrypt the message. This is why asymmetric cryptography was developed as a new way of encrypting messages.

Asymmetric cryptography resolves this problem by using two different but complementary keys. Messages encrypted with one key cannot be decrypted with the other. This allows for secure communication between parties who do not know each other. The public key can be distributed to all participants in the network, while the private key must be kept secret. This way, anyone can encrypt a message with the recipient's public key, but only the recipient can decrypt it using the corresponding private key.

Asymmetric cryptography also allows for digital signatures. A message encoded with a private key can only be decrypted with the corresponding public key. This ensures the authenticity of the message. It is still possible to use symmetric encryption for performance reasons, but asymmetric encryption is used for its security benefits.

In conclusion, encryption and cryptography are essential tools for protecting digital information. While symmetric cryptography is simpler and faster, asymmetric cryptography provides stronger security and is more versatile. Both methods have their strengths and weaknesses, and the choice of which to use depends on the specific needs and requirements of the situation.
As time went by, it appeared that the reverse direction had advantageous applications. The sender can unequivocally identify himself/herself as the author of his/her messages by encrypting them with his/her private key. Everyone can use the public key to verify the origin and integrity of the messages. These characteristics make asymmetric cryptography an excellent electronic substitute for the handwritten signature.

### 3. SIGNING A MESSAGE

A digital signature is created as follows:

1. A hashing algorithm is used to calculate the fingerprint of the message to be signed.
2. The sender encrypts the hashing code with his own private key. The result is called the “digital signature.”
3. The digital signature is added to the document and sent with it to the recipient.
4. It is not necessary to encrypt the complete message; only the hashing code need be encrypted, which requires much less calculating power.

### 4. VERIFYING THE SIGNATURE

The recipient must verify the sender’s digital signature to determine the originator of the document. This is how it is done:

1. The recipient calculates the hashing code for the message received.
2. The digital signature sent with the document is an encrypted hashing code that matches the fingerprint of the message received. The digital signature is successfully verified when these two values are identical.
3. The recipient can now be certain about the integrity of the message and the identity of the sender. The owner of the private key that corresponds to the public key used is identified to the extent that the recipient knows with certainty who the owner of this key pair is.
5. PUBLIC KEY INFRASTRUCTURE

The digital signature identifies the sender of a message only relatively. The recipient must learn in one way or another who owns the public key used to verify the signature. Since the private key is inseparable from the public key, there is no way to determine who sent the message without knowing the private key. The digital signature provides assurance only if the private key is associated with the right person.

The certificate holder can include a copy of the certificate with his digital signature. This allows the recipient to verify the authenticity of the signature using the certificate.

Certificates explicitly establish the link between a public key and a specific person. They can be compared to identity cards. In principle, anyone can hand out such certificates stating the link between a public key and a specific person in a document, which is then signed. Third parties will consider such a certificate credible to the extent that they have confidence that the certificate issuer is telling the truth. This solution is sufficient within small circles, but it is not practicable on a large scale.

That is why specialized companies offer their services as independent “trusted third parties” (TTP) that grant certificates to anyone who asks for them. These companies are called “Certificate Authorities” (CA), even though they are often private companies.

The CA establishes the link between a person and a public key in a certificate. Organizations as well as natural persons can own a public key. Depending on the desired level of certificate security, the CA verifies the accuracy of the identification data supplied by the certificate holder.

A low-level certificate may mention only a pseudonym. To obtain an advanced certificate, the CA can require the owner of the public key to present himself/herself to the CA before the certificate is issued. Certificate verification is done by using the CA’s public key, just as the digital signature is verified using the certificate holder’s private key.

The certificate holder can include a copy of the certificate with his digitally signed message. The recipient of the digital information can verify the certificate using the CA’s public key, just as the digital signature is verified using the certificate holder’s private key.
element in the security of the ICT environment. Management, certificate management, access to registers, etc., play an important role in this context. Cryptography can be implemented in a variety of services based on public key infrastructure (PKI), which consists of a combination of hardware, software, and procedures. A framework within which a variety of services based on public key cryptography can be implemented. It is clear that a whole infrastructure is needed in addition to the key pairs issued by the CA. The link between the public key and the identity is established in the certificate issued by the CA. The public key for this reason the CA's public key must be disclosed if allows the recipient to be certain which CA issued the certificate. When he trusts the CA, he will accept the certificate.
A. INTRODUCTION

The DAVID-project examined how electronic records can be archived in a durable and reliable way. Long-term archiving of electronic records is a challenge for a variety of reasons and has a number of obstacles to overcome. These will be summarised one-by-one below, so it becomes clear what solutions are needed for electronic record keeping. Since the DAVID-research primarily focused on electronic records, it is useful to examine our study object more closely in the second section of this chapter. This is the starting point from which the broad range of problems and issues concern electronic archiving in general (section 3).

1. PROBLEMS AND ISSUES?

1.1. THE TECHNOLOGICAL OBSOLESCENCE

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.2. THE LARGE QUANTITY OF DOCUMENTS

Agencies are making full use of IT facilities for the creation and exchange of documents. The quantity of digital documents is increasing every day. Even when archival records are electronic, it is a problem that there is a large number of documents. Records managers are increasingly confronted with the storage and archiving of electronic documents.

1.3. THE APPRAISAL AND SELECTION PROCESS

Administrative staff members and public servants are responsible for the appraisal and selection process when electronic records are created. Electronic records are not self-evident and require a number of special activities and specific security measures. It is essential that managers, records managers and archival staff are aware of these issues.

1.4. THE AUTHENTICITY AND RELIABILITY OF RECORDS

An electronic record should be as reliable as a traditional record. This is not the case, since there is a risk that an electronic record may be altered or destroyed. Records managers are increasingly confronted with the problem of ensuring the reliability of electronic records.

1.5. THE VARIETY OF DOCUMENTS

Electronic records are not self-evident. A number of special activities and specific security measures are essential when electronic records are created.

1.6. THE ARCHIVING OF THE CONTEXT

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.7. THE RETRIEVAL AND THE ACCESSIBILITY

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.8. THE AUDITABILITY OF RECORDS

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.9. THE ARCHIVAL AND THE ACCESSIBILITY

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.10. THE SECURITY OF RECORDS

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.11. THE AUTHENTICITY AND RELIABILITY OF RECORDS

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.12. THE VARIETY OF DOCUMENTS

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.13. THE ARCHIVING OF THE CONTEXT

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.14. THE RETRIEVAL AND THE ACCESSIBILITY

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.15. THE AUDITABILITY OF RECORDS

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.16. THE SECURITY OF RECORDS

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.17. THE AUTHENTICITY AND RELIABILITY OF RECORDS

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.18. THE VARIETY OF DOCUMENTS

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.19. THE ARCHIVING OF THE CONTEXT

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.

1.20. THE RETRIEVAL AND THE ACCESSIBILITY

Electronic records are by definition digital. A certain hard- and software configuration is required for accessing and viewing digital documents. One must depart from the principle that records will have a longer lifespan than the hardware and software on which they were created or managed. Therefore, a solution for technological obsolescence must be available. An electronic record cannot after all have a very long term archival value unless the hardware on which the raw data are stored retains for a very long period its technical functionality. In practical terms this means that an electronic record can only be stored in an electronic format for as long as there is software available that can access it.
1.3. THE APPRAISAL AND SELECTION PROCESS

Electronic records management systems and the digital repository may also maintain control over the functional requirements for the infrastructure of electronic records management. Appraisal and selection, however, are critical. The accessibility of electronic records that have already been created and released is one of the main challenges. Appraisal is the key for managing electronic records that have been created in complex and technology-dependent systems. Appraisal also plays a role in the choice of certain file formats as archiving file formats.

1.4. THE VARIETY OF DOCUMENTS

Digital documents that are currently being created and received, are of a highly diverse nature. There is not only a high diversity of object types (word processing files, spreadsheets, e-mails, databases, images, audio-visual materials, websites, GIS, CAD, virtual models, etc.), also the hard- and software configurations vary greatly. An appropriate archiving solution is necessary for each electronic record. This is often a very complex and technology-dependent process, which requires extensive research, time and resources. Selection and appraisal, however, are critical. Appraisal is the key for managing electronic records that have been created in complex and technology-dependent systems. Appraisal is also necessary for the choice of certain file formats as archiving file formats.

1.5. THE AUTHENTICITY AND RELIABILITY OF RECORDS

Electronic records have the advantage that they can always be changed after their creation. They can be modified very quickly. But, the contents of records must be fixed and unalterable. In many cases, a change in a digital document cannot be detected afterwards. This can lead to doubts about their reliability, and is why appropriate measures are needed. Appraisal is the key for managing electronic records that have been created in complex and technology-dependent systems. Appraisal is also necessary for the choice of certain file formats as archiving file formats.
1.6. THE ARCHIVING OF THE CONTEXT

Digital documents depend on the computer configuration and the user settings. Digital objects have different appearances when viewing on screen or on paper. The original document cannot be differentiated from the copied document. Computer equipment and software are available to render electronic records into their conceptual form. The representation of records is based on the document's conceptual representation. Changes and alterations are evident in the digital record. Therefore, a more explicit identification and description of each electronic record are necessary.

Electronic records differ in several respects from paper records. A number of important differences are caused by the fact that electronic records are digital objects:

- The way in which a digital object is stored and displayed is not the same as the way it is used.
- Electronic records differ in several respects from paper records. A number of important differences are caused by the fact that electronic records are digital objects:

2. THE ELECTRONIC RECORD

Electronic records differ in several respects from paper records. A number of important differences are caused by the fact that electronic records are digital objects:

- The storage medium and the archival record are no longer in unified changes.
- The storage medium and the archival record are no longer in unified changes.

Electronic records differ in several respects from paper records. A number of important differences are caused by the fact that electronic records are digital objects:

- Electronic records differ in several respects from paper records. A number of important differences are caused by the fact that electronic records are digital objects:
The look and feel of the same record isn’t always the same. Electronic records can also have different bit representations: the same record (for instance an e-mail message) can be stored in different formats (for instance MSG, ASCII/Unicode, TIFF, PDF, XML, etc.) and therefore in different bitstreams. There is no fixed relationship between electronic records and computer files; therefore, making a clear distribution necessary. The relationship between electronic records and computer files can be affected by the configuration and the settings of the operating system depending on the computer configuration. The rendering on screen of the same bitstream will be given a new representation depending on the computer configuration. The rendering on screen may not be only through technological obsolescence. Actually, everything a digital document appears like through technological obsolescence actually everything a digital document appears like through technological obsolescence. After all, the original does not survive in a digital world. The original is doomed to disappear, if only through technological obsolescence. The rendering on screen of the same bitstream will be given a new representation depending on the computer configuration. The rendering on screen may not be only through technological obsolescence. Actually, everything a digital document appears like through technological obsolescence.
Digital archiving

**Part 2: Electronic Record Keeping**

Electronic records are, on the other hand, also more than just digital objects. They need to be executable, understandable, and must be able to be used as records. They need to be executable, understandable, and must be used as electronic records. This leads to three requirements that the record must fulfill:

1. **Fixed documentary form**: The structure, composition, and defined rendering of the document.
2. **Static or fixed content**: The content is immutable.
3. **Context**: The archival bond with the records creator, with the business process in which they were created or received, together with related records.

In general, five components are differentiated in an electronic record:

- **Content**
- **Structure**
- **Context**
- **Layout**, "look and feel"
- **Behavior**, functionality.

The identification of records and their appraisal results in a definition of the essential and incidental properties or components of a record. The content, structure, and context of the record are essential components. By contrast, the "look and feel" and the behavior are not always essential for the record's authenticity. They imply that the record may be lost or changed intuitively, resembling a photo record.

The essential properties must be archived in an unaltered way, while the incidental properties may be lost or changed. The final purpose of the document may not have been changed and that the essential components are complete and correct. The goal of digital archiving is to transmit an understandable electronic record over time.

### 3. Digital Archiving

The goal of digital archiving is to transmit an interpretable electronic record over time.

- **Executable**: The digital storage media must contain intact bitstreams and it must be possible to transfer these to the computer's memory.
- **Renderable**: The bitstreams must be processed correctly by the computer, so that the record can be displayed on screen.
- **Understandable**: The digital storage media must contain intact bitstreams and a static or fixed content.

The goal of digital archiving is to transmit an understandable electronic record over time.

- **Behavior**, functionality
- **Evolve, look, and feel**
- **Context**
- **Structure**
- **Content**
Digital archiving

Part 2: Electronic Record Keeping

80

4. CONCLUSION

Electronic records are no longer interpretable, or even usable, if one of its initial recipients
records are not the authors, nor one of its initial recipients
from contact with the digital nature of electronic records.
From the point of view of administrative metadata, in most cases the user of electronic records
must be able to identify the documents within the document hierarchy, who are capable of using those documents without additional knowledge. The support of the application software is also necessary at the end of the process of the first interpretation, where backups are applied to the electronic records. When the documentation is the digital record, the backup medium in the short-term, while electronic records must be kept. If the same is made, a backup copy? The goal of backup copies is to repair lost or damaged documents, and it must be considered as lost if any one of these sequential steps is missing. The greater the number of dependencies, the greater the risk is of losing records. For these reasons, elements such as backup formats, compression and encryption should be avoided as much as possible.

The characteristics of an electronic record also show that digital archiving is no longer interpretable, and it must be considered as lost if the meaning of the document is not understood. The user, so that he/she can only access the function of the record that was created at the same time the document was created. Nevertheless, the application software supports the function of the electronic record, if necessary, additional metadata can be attached to the electronic records, and they will be displayed on the screen. This is only possible when there are no losses of the electronic record.

The electronic record is no longer interpretable, or even usable, if one of its initial recipients is not the user of the document. From contact with the digital nature of electronic records. The user must be able to identify the documents within the document hierarchy, who are capable of using those documents without additional knowledge. The support of the application software is also necessary at the end of the process of the first interpretation, where backups are applied to the electronic records. When the documentation is the digital record, the backup medium in the short-term, while electronic records must be kept. If the same is made, a backup copy? The goal of backup copies is to repair lost or damaged documents, and it must be considered as lost if any one of these sequential steps is missing. The greater the number of dependencies, the greater the risk is of losing records. For these reasons, elements such as backup formats, compression and encryption should be avoided as much as possible.

The characteristics of an electronic record also show that digital archiving is no longer interpretable, and it must be considered as lost if the meaning of the document is not understood. The user, so that he/she can only access the function of the record that was created at the same time the document was created. Nevertheless, the application software supports the function of the electronic record, if necessary, additional metadata can be attached to the electronic records, and they will be displayed on the screen. This is only possible when there are no losses of the electronic record.

The electronic record is no longer interpretable, or even usable, if one of its initial recipients is not the user of the document. From contact with the digital nature of electronic records. The user must be able to identify the documents within the document hierarchy, who are capable of using those documents without additional knowledge. The support of the application software is also necessary at the end of the process of the first interpretation, where backups are applied to the electronic records. When the documentation is the digital record, the backup medium in the short-term, while electronic records must be kept. If the same is made, a backup copy? The goal of backup copies is to repair lost or damaged documents, and it must be considered as lost if any one of these sequential steps is missing. The greater the number of dependencies, the greater the risk is of losing records. For these reasons, elements such as backup formats, compression and encryption should be avoided as much as possible.

The characteristics of an electronic record also show that digital archiving is no longer interpretable, and it must be considered as lost if the meaning of the document is not understood. The user, so that he/she can only access the function of the record that was created at the same time the document was created. Nevertheless, the application software supports the function of the electronic record, if necessary, additional metadata can be attached to the electronic records, and they will be displayed on the screen. This is only possible when there are no losses of the electronic record.

The electronic record is no longer interpretable, or even usable, if one of its initial recipients is not the user of the document. From contact with the digital nature of electronic records. The user must be able to identify the documents within the document hierarchy, who are capable of using those documents without additional knowledge. The support of the application software is also necessary at the end of the process of the first interpretation, where backups are applied to the electronic records. When the documentation is the digital record, the backup medium in the short-term, while electronic records must be kept. If the same is made, a backup copy? The goal of backup copies is to repair lost or damaged documents, and it must be considered as lost if any one of these sequential steps is missing. The greater the number of dependencies, the greater the risk is of losing records. For these reasons, elements such as backup formats, compression and encryption should be avoided as much as possible.

The characteristics of an electronic record also show that digital archiving is no longer interpretable, and it must be considered as lost if the meaning of the document is not understood. The user, so that he/she can only access the function of the record that was created at the same time the document was created. Nevertheless, the application software supports the function of the electronic record, if necessary, additional metadata can be attached to the electronic records, and they will be displayed on the screen. This is only possible when there are no losses of the electronic record.

The electronic record is no longer interpretable, or even usable, if one of its initial recipients is not the user of the document. From contact with the digital nature of electronic records. The user must be able to identify the documents within the document hierarchy, who are capable of using those documents without additional knowledge. The support of the application software is also necessary at the end of the process of the first interpretation, where backups are applied to the electronic records. When the documentation is the digital record, the backup medium in the short-term, while electronic records must be kept. If the same is made, a backup copy? The goal of backup copies is to repair lost or damaged documents, and it must be considered as lost if any one of these sequential steps is missing. The greater the number of dependencies, the greater the risk is of losing records. For these reasons, elements such as backup formats, compression and encryption should be avoided as much as possible.

The characteristics of an electronic record also show that digital archiving is no longer interpretable, and it must be considered as lost if the meaning of the document is not understood. The user, so that he/she can only access the function of the record that was created at the same time the document was created. Nevertheless, the application software supports the function of the electronic record, if necessary, additional metadata can be attached to the electronic records, and they will be displayed on the screen. This is only possible when there are no losses of the electronic record.

The electronic record is no longer interpretable, or even usable, if one of its initial recipients is not the user of the document. From contact with the digital nature of electronic records. The user must be able to identify the documents within the document hierarchy, who are capable of using those documents without additional knowledge. The support of the application software is also necessary at the end of the process of the first interpretation, where backups are applied to the electronic records. When the documentation is the digital record, the backup medium in the short-term, while electronic records must be kept. If the same is made, a backup copy? The goal of backup copies is to repair lost or damaged documents, and it must be considered as lost if any one of these sequential steps is missing. The greater the number of dependencies, the greater the risk is of losing records. For these reasons, elements such as backup formats, compression and encryption should be avoided as much as possible.

The characteristics of an electronic record also show that digital archiving is no longer interpretable, and it must be considered as lost if the meaning of the document is not understood. The user, so that he/she can only access the function of the record that was created at the same time the document was created. Nevertheless, the application software supports the function of the electronic record, if necessary, additional metadata can be attached to the electronic records, and they will be displayed on the screen. This is only possible when there are no losses of the electronic record.

The electronic record is no longer interpretable, or even usable, if one of its initial recipients is not the user of the document. From contact with the digital nature of electronic records. The user must be able to identify the documents within the document hierarchy, who are capable of using those documents without additional knowledge. The support of the application software is also necessary at the end of the process of the first interpretation, where backups are applied to the electronic records. When the documentation is the digital record, the backup medium in the short-term, while electronic records must be kept. If the same is made, a backup copy? The goal of backup copies is to repair lost or damaged documents, and it must be considered as lost if any one of these sequential steps is missing. The greater the number of dependencies, the greater the risk is of losing records. For these reasons, elements such as backup formats, compression and encryption should be avoided as much as possible.

The characteristics of an electronic record also show that digital archiving is no longer interpretable, and it must be considered as lost if the meaning of the document is not understood. The user, so that he/she can only access the function of the record that was created at the same time the document was created. Nevertheless, the application software supports the function of the electronic record, if necessary, additional metadata can be attached to the electronic records, and they will be displayed on the screen. This is only possible when there are no losses of the electronic record.

The electronic record is no longer interpretable, or even usable, if one of its initial recipients is not the user of the document. From contact with the digital nature of electronic records. The user must be able to identify the documents within the document hierarchy, who are capable of using those documents without additional knowledge. The support of the application software is also necessary at the end of the process of the first interpretation, where backups are applied to the electronic records. When the documentation is the digital record, the backup medium in the short-term, while electronic records must be kept. If the same is made, a backup copy? The goal of backup copies is to repair lost or damaged documents, and it must be considered as lost if any one of these sequential steps is missing. The greater the number of dependencies, the greater the risk is of losing records. For these reasons, elements such as backup formats, compression and encryption should be avoided as much as possible.
1. HARD COPY STRATEGY

1. Hard Copy Strategy

1. Hard Copy Strategy

2. Preservation of Technology

3. Conversion

4. Migration

5. Conclusion: Preservation of the original and the migrated bitstreams

In the hardcopy strategy, electronic records are transferred to microfilm or printed out on paper. However, the same holds for records created in paper form. In a conversion to paper or microform, it is advisable to transfer the electronic version to external media, if possible, and the version created digitally will be archived digitally. However, archival science processes from the principle that records should be understood correctly.

Electronic records are digital objects. Various strategies can be applied for the long-term preservation of a digital object. Below we will discuss the most common strategies that can be applied for the long-term preservation of electronic records. The following preservation strategies are discussed:

1. Hard Copy Strategy

2. Preservation of Technology

3. Conversion

4. Migration

5. Conclusion: Preservation of the original and the migrated bitstreams
For medium-term and long-term storage, this solution is not feasible. For this reason alone the hard-copy strategy is not advisable.

**2.1 COMPUTER MUSEUM STRATEGY**

Preservation of Technology

An important requirement is that all essential information will be included on the records. A conversion to paper or microfilm can only be considered as a temporary archiving solution, which is applied in expectation of a full electronic record keeping procedure. This option is by the way not applicable to all types of digital documents. An important requirement is that all essential information will be included on the printout or the microfilm version.

**A printout on paper or a transfer to microfilm can only be considered as a temporary archiving solution.**

An important characteristic of a digital document is that a transfer to new storage media is necessary.

- records on paper are more expensive than digital archives.
- higher costs for conversion to paper or microfilm and the storage of paper.
- not all electronic records can be transferred to paper or microfilm (for instance GIS, CAD, multimedia objects, databases).
- not all essential information is always printed out.
- a primary copy in business processes.
- new storage media will probably not be compatible with the old computer configurations.
- a transfer of electronic records to new storage media becomes necessary.
- all essential characteristics of a digital document is lost, namely its "digital nature". For this reason alone the hard-copy strategy is not advisable.
This approach is only possible for short-term storage (5 to 10 years) of electronic records. The museum strategy is therefore only usable for the storage of those records, where the archival value does not exceed the lifespan of the technology, or as a temporary solution if expectations of a more permanent record keeping strategy is high. In such a case, the museum strategy is only applicable if the museum records its own electronic records.

2.2 EMULATION

In the emulation strategy, the original hardware is not preserved. Instead, the required platform is emulated on future (newer) computer configurations, so that electronic records can be consulted in their original (obsolete) file format.

Emulation has a number of interesting advantages:

- in theory, the documents can be preserved and accessed in their original format:
  - all original properties and functionalities are maintained
  - no elements are lost as a consequence of conversion or migration
  - the authenticity of the electronic records is easier to guarantee
- no external costs are associated with emulation of migration
- the cost is not dependent on the number of preserved electronic records

Emulation has a number of disadvantages:

- emulation is technically very complex and requires a great deal of know-how and expertise in digital archiving.

At the moment different views exist with regard to the way emulation can be applied.

Emulation can be applied at various levels:

- Emulation Virtual Machine (software)
- Emulation via hardware

In digital archiving, a number of interesting approaches can be distinguished:

- Cedars & Camileon project: Migration on request
- Raymond Lorie: Universal Virtual Machine (data preservation, program migration)
- Jeff Rothenberg: Emulation Virtual Machine
- Steve Gilheany: Turing Machine

In the emulation strategy, the original hardware and software are preserved instead of being replaced by newer versions. Computer programs (emulation via software) can be consulted in their original form. The required platform is emulated on newer (more powerful) computer configurations, so that electronic records can be consulted in their original format. The emulation approach is only applicable if the museum records its own electronic records.
Part 2: Electronic Record Keeping

The feasibility of certain emulation approaches will only become apparent in the future, and software and necessary documentation, innovations and new archiving technologies are not yet available. New, especially developed, software and additional documentation are needed for the maintenance of the original functionalities. Furthermore, archival institutions are only able to develop and test software. Emulation is not possible without software, which means that it is not possible to use old archival software. Emulation is not possible without new software, which can be developed by archival institutions. However, it is not possible to use old archival software without new software. Emulation is not possible without new software, which means that it is not possible to use old archival software. Emulation is not possible without new software, which means that it is not possible to use old archival software.

The protection of authors rights on electronic records is an essential task for archivists. In order to protect the original content, the protection of the original content is essential. The protection of the original content is essential. The protection of the original content is essential.

In the future, archivists and archives will be faced with many new challenges and tasks. Emulation is one of the most important strategies for the preservation of electronic records. In all events, the experience with emulation as a digital preservation strategy is limited at present. The present time learning about a large number of applications is necessary. Learning about a large number of applications is necessary. Learning about a large number of applications is necessary. Learning about a large number of applications is necessary. Learning about a large number of applications is necessary. Learning about a large number of applications is necessary. Learning about a large number of applications is necessary. Learning about a large number of applications is necessary.
In the case of conversion, digital documents are converted from a lower to a higher version of the same file format. An example is the conversion of a document that was created in MS Word 97 to MS Word 2000.

The advantages:
• the documents remain executable and fully functional.

The disadvantages:
• electronic records must be converted with a high frequency (for instance MS Word 6.0, MS Word 97, MS Word 2000, MS Word 2002, MS Word 2003).

Conversion is not a practical long-term storage strategy for digital documents. As a consequence, conversion should be avoided as much as possible, unless no other possibilities are available. For instance, when no suitable archiving format is available or if the loss of essential components of the record appears imminent.

Conversion is also not a practical long-term storage strategy for digital documents because:
• the document is more difficult to guarantee.
• the documents are not stored in an unambiguous and not dependent software format.
• the specification of the file format is not available.
• electronic records are not stored in an unambiguous software format.
• conversion tools are not available.

Migration is a preservation strategy in which digital documents are transformed into suitable archiving file formats. This is currently the most frequent method used for archiving electronic records.

The advantages of migration as a storage strategy are:
• electronic records are not stored in a manufacturer-, software- or version-dependent file format.
• the specification of the file format is available: on the basis of this format, documentation, a new viewer can be programmed at any time.
• the specification of the file format is available: on the basis of this format, documentation, a new viewer can be programmed at any time.

The disadvantages of migration as a storage strategy are:
• migration to a standardised format is sometimes also indicated by the terms, "normalisation" or "normalisation".
The disadvantages:

- this storage strategy is strongly depending on standards. However, standards have a number of disadvantages:
  - their development process takes a long time; this means that standards cannot follow the speed of the market evolution
  - standards are not always precisely applied or implemented: standards are sometimes expanded, so that additional functionalities become available, through which the documents are no longer fully compatible
  - standards support almost no application-oriented functionalities
  - not all standards are equally well distributed or have a sufficient market penetration
  - standards do not have an unlimited lifespan
  - for some file formats there are no suitable archiving file formats available
  - the original properties or functionalities of the source format can rarely integrally be transferred to the target format: migration is in many cases associated with loss.

Migration is at present the most frequently used strategy for the long-term preservation of electronic records. One must, however, make sure that no essential information is lost during migration, and that the authenticity of the electronic records is not compromised. In principle, this is no hindrance for the application of a migration strategy. With a thorough analysis of the source and the target format, such risks can be avoided and any loss that may occur during the migration process can be reduced and any loss that may occur during the migration process can be reduced.

The migration procedure should be automated, taking into account the large quantity of electronic records. Manual conversions are laborious and can be inconsistent. Automated migration procedures lead to a number of special requirements for the migration process. One must define a migration path for each record type. A migration path consists of the following steps:

1. appraisal and selection: identify the record and define the essential and incidental characteristics of the record
2. choice of the target file format
3. choose a file format that fulfills the requirements of a suitable archiving file format (see C.3.2)
4. choose a file format that supports all essential components of the electronic record
5. define the profile of the target file format (uncompressed, color schema, encapsulation of metadata, etc.)
6. pay attention to the encapsulated metadata in the source file.

For some file formats, there are suitable archiving file formats available. The migration strategy is strongly depending on standards. However, standards have a number of disadvantages.
Digital Archiving
Part 2: Electronic Record Keeping

5. CONCLUSION: PRESERVATION OF THE ORIGINAL AND THE MIGRATED BITSTREAMS

An evaluation of the possible preservation strategies shows that there are current no definitive solutions for the long-term preservation of electronic records. None of the discussed preservation strategies is free of risk. The search for a suitable preservation strategy has for many years focused on the software side. Evaluation strategies for a solution for the readability problem of archival documents must be available in addition to preservation strategies of the electronic record. The decision between migration and emulation can be based on the importance of the reproduction of the document. Emulation is more suitable when the look and feel of the document is important, whereas migration is preferable when the content is important.

A preservation strategy that is recommended by the DAVID-project is a middle way between migration and emulation. This is achieved by preserving the original bitstreams together with the migrated versions, which offers more guarantees towards long-term readability of the migrated versions. When we preserve the original bitstreams together with the migrated versions, we can achieve a direct solution for the readability problem. This can be achieved when we perform all actions open for the future within a framework of emigration and migration. Keeping all options open for the future is a mark of the preservation strategy that is recommended by the DAVID-project.
Part 2: Electronic Record Keeping

When the MS Word file is ingested into the digital repository, it is possible to store it in its original file format or in a suitable archiving file format before the ingest. The record in its original file format is not destroyed; instead, it is also included in the digital repository. This means that two representations of the same electronic record are preserved: one in its original file format, and one in the migrated file format. It is possible to store these representations in separate computer files, or to encapsulate them in one XML container. This offers the advantage that in the future both emulation and migration are possible, either from the original or from the migrated file format. No migration is necessary for electronic records, which were directly created in a suitable archiving file format, so only one representation of such record must be preserved.

When applied to a text document which had been saved in an MS Word format, this preservation strategy includes the following steps. At the latest at the time the document is ingested in the digital repository (moment x), the text document in an MS Word format will be migrated to a suitable archiving file format with migration tool A. Depending on an identification of the essential components and on appraisal, a selection will be made from the XML, TIFF and PDF archiving file formats. MS Word is after all an undocumented file format that is dependent upon one manufacturer and one application, for which only time-limited support is available, making it totally unsuitable for long-term archiving. In the digital repository, both the original MS Word file and the migrated file are stored. Whenever the XML, TIFF or PDF archiving file format is identified as obsolete (moment y), one has a choice between various options:

- the use of an emulator for the original file format
- the use of an emulator for the migrated file format
- migration to a new archiving file format (migrated bitstream 2), carried out on the MS Word file

If the original file format becomes obsolete before the migrated file format, this means that the digitization has been successful, and that the essential components of the former have been preserved in the latter. If the migrated file format becomes obsolete before the original file format, this means that the digitization has been successful, and that the essential components of the latter have been preserved in the former. If both file formats become obsolete simultaneously, this means that the digitization has been unsuccessful, and that the essential components of neither have been preserved in either.
are preferably applied so the electronic records are least exchangeable.

Even if, in the case of MS Word, emulation appears to be a relatively unlikely possibility, this preservation strategy could mean that more of the original properties of the record are preserved in the second archiving file format than in the first archiving file format.

1. IMPORTANCE

C. ARCHIVING STANDARDS

IT standards play an important role in every preservation strategy. In the case of migration, the record is preferably transformed to a standardised file format. This means that records do not need to be migrated since the technical specifications of the record can be programmed. Instead, the record is preserved in the second archiving file format. The record is preserved in the second archiving file format than in the first archiving file format. This is why preservation strategies such as the migration of MS Word emulation appears to be a relatively unlikely possibility.
Standards can be applied to:
• the preservation media on which the electronic records are stored
• the file formats in which the electronic records are stored.

2. PRESERVATION MEDIA

2.1. DURABLE STORAGE MEDIA

Whether electronic records will still be renderable in the future depends, in the first place, on the media on which they have been stored. Electronic records are best stored on durable preservation media. The preservation media must be capable of storing data for the long-term and may not deteriorate too quickly.

The lifespan of storage media is usually examined on the basis of tests, whereby the ageing process is speeded up and where the number of errors on the aged storage media are measured. The lifespan of the storage media is subsequently forecast on the basis of these tests, and on the assumption that the medium is stored under good conditions. An error-detection and error-correction system is taken into account in this examination. After all, the envisaged electronic records will still be readable in the future, depending on the basis of tests, whereby certain conditions must be met by the media.

The life expectancy of a certain storage medium into the computer's memory to load the information on a certain storage medium into the computer's memory must have access to the necessary hardware, and software in the future to be able to do this.

2.2. LIFE EXPECTANCY OF TECHNOLOGY

One must have access to the necessary hardware and software in the future to be able to load the information on a certain storage medium into the computer's memory.

The efficiency of the error-detection and error-correction system is examined on the basis of tests, whereby the number of errors on the aged storage media are measured, and the lifespan of the storage media is subsequently forecast on the basis of these tests.

The life expectancy of a certain storage medium into the computer's memory to load the information on a certain storage medium into the computer's memory must have access to the necessary hardware, and software in the future to be able to do this.
PART 2: ELECTRONIC RECORD KEEPING

2.3. GENERAL RECOMMENDATIONS

Both magnetic and optical storage media, in practice, used as preservation medium and a durable technology, the frequency of refreshing operations can be reduced to a minimum.

2.4. MAGNETIC PRESERVATION MEDIA

More information and practical recommendations are available on the DAVID-website:

2.4. GENERAL RECOMMENDATIONS

- Magnetic and optical storage media, in practice, used as preservation medium and a durable technology, the frequency of refreshing operations can be reduced to a minimum.

2.3. GENERAL RECOMMENDATIONS

Both magnetic and optical storage media, in practice, used as preservation medium and a durable technology, the frequency of refreshing operations can be reduced to a minimum.
Recommendation: be careful when using hard disks as a medium for long-term storage!

- use a type of hard disk that has proven its durability
- make sure that safety procedures against data loss are available (for instance RAID 5)
- hard disks are not durable; they have a relatively short life expectancy (due to heat, wear and tear)
- folders and files are saved in a filesystem that is defined by a certain type of operating system; a duplicate storage in two different types of filesystems (for instance Windows and Unix/Linux) gives extra security
- writable DVDs are not easily exchangeable
- the standardisation of DVD technology has not been completed yet
digital archiving: do not use DDF as a long-term preservation medium!

Recommendation: do not use backup tapes for archiving purposes!

- backup tapes are usually compressed: specific software is required for decompression
- backup files are usually compressed: specific software is required for decompression
- not all information that is required for the reconstruction of computer files is necessarily stored on the storage medium. Certain, essential information is maintained on a backup computer
- backup tapes serve short-term file recovery goals, and not long-term preservation of digital records
- backup tapes do not provide administrative or technical metadata about the context of the records
- backup tapes serve short-term file recovery goals, and not long-term preservation of digital records


table of optical preservation media

<table>
<thead>
<tr>
<th>Medium</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Durable CD's</td>
<td>Durable, reliable, long-term preservation</td>
</tr>
<tr>
<td>Writable DVDs</td>
<td>Not easy to exchange, limited durability</td>
</tr>
</tbody>
</table>

Durable CD's

More information and practical recommendations are available on the DAVID-website:

- Digital Archiving Guideline & Advice, no. 2: Durable CD's
- F. Boudrez, CDs voor het archief: Archieven van heden, Antwerp, 2001

Recommendation: do not use DVD as a long-term preservation medium!

- the standardisation of DVD technology has not been completed yet: different standards exist beside each other
- writable DVDs are not easily exchangeable
- the standardisation of DVD technology has not been completed yet

3. FILE FORMATS

Electronic records are preferably stored in a standardised file format. As a rule, standardised file formats are:

- readable, exchangeable
- available on different operating systems
- not dependent on specific software
- not dependent on specific hardware
- not dependent on specific application software

For long-term storage:

Recommendation: be careful when using hard disks as a medium for long-term storage!
Digital archiving is the process of storing and managing data in a manner that ensures its availability, reliability, and authenticity over a long period. There are several criteria for suitable archiving file formats:

- **Open and documented**: their technical specifications are available. One can assume that viewers can easily be programmed when the technical specification of the file format is available.
- **Stable**: standards can only be revised when a certain procedure has been observed.
- **Software independent**: the standards are supported by different software applications and open source initiatives.
- **Manufacturer independent**.

### 3.1. HIERARCHY

A large number of different standards exist in the IT world, and a hierarchical structure can be used to manage and select the most suitable standards. The hierarchy is important for selecting a suitable archiving file format. When choosing a hierarchy, it is preferable to concentrate on official standards and specifications. The hierarchy is non-exclusive. The status of official standard does not in itself give any guarantee for instance criteria, and the hierarchy is an important guideline but is not the be-all and end-all. The following guidelines are recommended:

- **Official standards**: these are standards that have been defined by standardisation organisations. They are usually managed by a standardisation institute. The official standards are publicly documented and their management is in the hands of a manufacturer, but the technical specifications are open. The official standards are located at the top of the hierarchy. Examples are ISO (International Organisation for Standardisation), IEC (International Electrotechnical Commission) and ITU (International Telecommunications Union).

- **De facto standards**: these are standards that have been developed by non-official standardisation initiatives (for instance W3C). Their management is not in the hands of a manufacturer, but the technical specifications are not open. The de facto standards are situated below the official standards. The de facto standards can be subdivided into three subgroups:
  - **Open formats**: these are standards that have been developed by non-official standardisation initiatives. Their management is not in the hands of a manufacturer, but the technical specifications are open. Examples are XML (eXtensible Markup Language) and SGML (Standard Generalised Markup Language).
  - **Closed formats**: these are standards that have been developed by a manufacturer. Their management is in the hands of a manufacturer, but the technical specifications are open. Examples are PDF (Portable Document Format) and Microsoft Word.
  - **Proprietary formats**: these are standards that have been developed by a manufacturer. Their management is in the hands of a manufacturer, but the technical specifications are closed. Examples are Microsoft Excel and Adobe PDF.

When selecting a suitable archiving file format, it is preferable to concentrate on official standards and specifications. The hierarchy is an important guideline, but it is not the be-all and end-all. The status of official standard does not in itself give any guarantee. For instance, certain specifications are more widely applied than their official equivalents (for example, Unicode vs. ISO-10646; XML vs. SGML). Next to the degree of standardisation, there are still other criteria that are valid for suitable archiving file formats.
3.2. SUITABLE ARCHIVING FILE FORMATS

A suitable archiving file format preferably meets the following criteria:

- Standardised: documented, stable and not depending on one manufacturer
- Widely distributed with sufficient market penetration
- Exchangeable: independent of certain operating systems, network protocols and applications
- Storage without information loss (no lossy compression)
- Well-structured storage of information
- Possibilities for automatic and automated validation
- Possibilities for syntactic error detection and error-correction mechanism: errors in bit storage are repairable
- Provides a robust error-detection and error-correction mechanism: errors in and applications
- Exchangeable: independent of certain operating systems, network protocols
- Standardised: documented, stable and not depending on one manufacturer
- Autonomous and self-containing
- User-friendly
- Possibilities for media and equipment independent storage

These criteria are important in the choice of a certain file format as the archiving file format. It is also best to remember these quality requirements when applying.
archiving standards. Standards can, after all, be applied in various ways. Most archiving file formats make it possible for the user to define a number of settings and parameters. For instance, one can create a number of different types of TIFF, XML and PDF files, but not every TIFF, XML or PDF document is suitable for long-term preservation. JPEG compression can for instance be applied to images that are stored as TIFF files. Not only data is lost during this process, but one is also dependent on the corresponding decompression for a reconstruction. The quality of XML documents depends on the granularity, the nesting and semantics of the XML-tags. PDF documents that are destined for long-term preservation are preferably tagged, or at least structured.

It is best to keep electronic records as autonomous as possible. The dependencies for a reconstruction are preferably limited to an absolute minimum. The lack of a single necessary link in the reconstruction process can, after all, lead to the loss of the record. This is the reason why compression, encryption, passwords or other security settings should be avoided as much as possible.

Recommendation: do not use compression for long-term preservation!

Any dependencies are avoided to a maximum degree.

For certain types of digital information, no suitable archiving file formats are (as yet) available. These digital documents are so closely linked to the hard- and software environment in which they were created that they can only barely (or not at all) be used outside the environment in which they were created. In such a case, it is recommended to search for a form of which is used outside the environment. This is the case for certain types of multimedia objects at the present time. In such a case, it is recommended to search for a form of which is used outside the environment. This is the case for certain types of multimedia objects at the present time.

Recommendation: do not use compression for long-term preservation!

Any dependency should be avoided as much as possible.

For certain types of digital information, no suitable archiving file formats are (as yet) available. These digital documents are so closely linked to the hard- and software environment in which they were created that they can only barely (or not at all) be used outside the environment in which they were created. In such a case, it is recommended to search for a form of which is used outside the environment. This is the case for certain types of multimedia objects at the present time.
If compression is unavoidable, then one should opt for lossless compression, which does not alter the original data. Using lossless compression methods ensures that the data can be accurately restored to its original form.

3.3. EXAMPLES OF SUITABLE ARCHIVING FILE FORMATS

<table>
<thead>
<tr>
<th>Archiving File Format</th>
<th>Type of Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>MXF</td>
<td>Video:</td>
</tr>
<tr>
<td>GIF</td>
<td>GIF:</td>
</tr>
<tr>
<td>DXF</td>
<td>CAD:</td>
</tr>
<tr>
<td>WAV (uncompressed PCM)</td>
<td>Sound:</td>
</tr>
<tr>
<td>CMY</td>
<td>Screen and Vector</td>
</tr>
<tr>
<td>SVG</td>
<td>Vector</td>
</tr>
<tr>
<td>TIFF</td>
<td>Screen</td>
</tr>
<tr>
<td>PNG</td>
<td>Image:</td>
</tr>
<tr>
<td>ASCII, UNICODE, TEXT</td>
<td>Text:</td>
</tr>
</tbody>
</table>

Recommendations:
- Limit the number of file formats that are used within the organisation.
- If possible, store electronic records immediately after their creation in a suitable archiving file format.
- Do not preserve electronic records in a closed or undocumented format.
- Avoid the use of compression techniques such as ZIP, LZW, and others.
- Do not wrap up records into compressed formats (e.g., .zip, .tar, .rar).
- Whenever the original formats are not saved, destroy the original computer files.
- Whenever the original formats are saved, destroy the original computer files.
- Check that the standards are applied correctly and that the data is correctly encoded.
- Check that the migration has been checked and validated.
- Check that the electronic records are preserved.

ARCHIVING POLICY

1. ARCHIVING POLICY

D. POLICY AND PROCEDURES

Every organisation needs a general policy which defines the basic options and the goal of the record keeping procedure within the organisation. This policy must make clear the roles and responsibilities of different parties involved in the record keeping process. It should also spell out the mechanisms for the management and administration of records. The policy should be developed in consultation with all relevant stakeholders and should reflect the organisation's mission, values, and objectives. The policy should be reviewed and updated regularly to ensure its relevance and effectiveness.
2. THE OPEN ARCHIVAL INFORMATION SYSTEM (OAIS) MODEL

The Open Archival Information System (OAIS) model can be used as a guide in the development of an information management and record keeping system. OAIS was developed by the Consultative Committee of NASA for their Space Data Systems, and in the meantime it is established as an ISO standard (ISO 14721-2003). Although the OAIS model is applicable to both paper and electronic records, the model is primarily directed towards the second category.

The OAIS model is not a system model for a record keeping system which can be implemented immediately, but it is a conceptual reference model that offers a frame which can be used as a guide in the development of a long-term archiving policy. The OAIS model is a conceptual reference model that offers a frame which can be used as a guide in the development of a long-term archiving policy.

The OAIS model is a conceptual reference model that offers a frame which can be used as a guide in the development of a long-term archiving policy.
circumstances, refreshing of preservation media, error-detection (checksums), disaster plans, the preparation of backups, the maintenance of readability, etc.

• assuring accessibility (logical management): creation and updating of archival descriptions and metadata, and the provision of retrieval paths

• management: defining a policy, consultation with the archive creators, choosing standards, management of the digital repository, maintenance of documentation, follow-up on technological changes, etc.

• providing access to the archives and the records.

These five functions are the key processes in every record keeping procedure for electronic records, and they cover the entire document flow between the creator and the users of the archives. How these processes will look like, depends on the concrete design and realization of the record keeping procedures.

3. TOWARDS A CONCRETE RECORD KEEPING PROCEDURE

The record keeping policy and the archiving function within an organisation are put into practice through concrete archiving procedures.

A variety of archiving procedures are applicable for the archiving of electronic records.

3.1. GENERAL CRITERIA FOR AN ARCHIVING PROCEDURE

In general there are three types of criteria which a record keeping procedure must meet:

• legal: the legal framework in which a record keeping procedure operates, must be applicable for each type of record.

• archival science: the electronic records must conform to a number of archiving quality requirements such as a digital durability, the highest possible assurance that the electronic records are accessible, etc.

• implementation: the technological infrastructure, scalability, user-friendliness, etc.
A preliminary study will provide criteria to which the record keeping procedure must comply. The possible archiving solutions are further defined by each group of criteria. So that the record-keeping procedure can be practically defined in the next phase.

### 3.2. The DAVID-Decision Model

The DAVID-decision model can be used as a guideline in this regard. This decision model can be applied to the record-keeping procedure and further defined in a following step. The DAVID-decision model consists of four questions that can be answered on the basis of the information system in which the records are created, received or managed.

- **WHAT** is to be archived?
- **WHEN** is a record-keeping action carried out?
- **WHO** archives?
- **HOW** are record-keeping actions put into practice?

Concrete choices are made on the basis of this decision model, which forms the basis for answering these four questions.
3.2.1. WHAT is to be archived?

- Identification of records:
  - What are the records?
  - Which elements identify the documents that have a permanent archival value? What identifies the record: filename, unique ID number, etc?
  - Which components of the record are (permanently) preserved: content, structure, context, layout/look & feel, behaviour/functionalities?

  ➪ What are the essential and incidental properties of a electronic record?
  ➪ Which components give a document the status of a record?

- Will records be stored in their original file format, or are they only stored in their archiving file format?
- Are specific computer programs required for the reconstruction of the records (for instance emulation programs)?
- Which descriptive or technical metadata of the record will be archived?
- Which descriptive or technical metadata of the information system will be archived in which the record was created and/or managed?

3.2.2. WHO archives?

- Who creates the digital files?
- Who registers the descriptive metadata?
- Who registers the technical metadata?
- Who converts the documents to an archiving file format?
- Who deposits the records with the archival service?
3.2.3. HOW are record keeping actions put into practice?

- Which storage strategy will be used for digital objects:
  - Migration?
  - Emulation?
  - A combination of migration and emulation?

- In which archiving file format will documents be saved and preserved?

- How will the metadata be archived:
  - In a separate computer file?
  - Embedded in the same computer file that contains the record?
  - In a separate computer file?

- Which instruments/tools are used for the registration of the metadata and the conversion to archiving file formats?

- How will the old electronic records be archived? What tools are required in this regard?

- How are the records and their metadata deposited at the archival service?

- On what type of preservation media will the records and their metadata be stored?

- How will the authenticity and the integrity of the archived digital documents be guaranteed?

- How will the capacity of the storage system be guaranteed?

- How will the retention period of the documents be guaranteed?

- How will the performance level of the computer system be guaranteed?

- How will the product support of the computer system be guaranteed?

- How will the replacement of the computer system be guaranteed?

- How will it be guaranteed that records are not changed after they have been stored?

3.2.4. WHEN is a record keeping action carried out?

- When will the record be stored? When is the record created? When is the record given the status and function of a record?

- Which steps in the archiving procedure are carried out at what time?

- When were the records transferred to the archival service?

- When does registration take place?

- How will the metadata be archived?

- In what type of preservation media will the records and their metadata be stored?

- Which instruments/tools are used for the registration of the metadata and the conversion to archiving file formats?

- In which archiving file format will documents be saved and preserved?

- How are the records and their metadata deposited at the archival service?

- On what type of preservation media will the records and their metadata be stored?

- How will the authenticity and the integrity of the archived digital documents be guaranteed?

- How will it be guaranteed that records are not changed after they have been stored?

Parameters:

- Capacity of the storage system
- The retention period of the documents
- The performance level of the computer system
- Product support of the computer system
- Replacement of the computer system
- The protection of personal privacy create limitations?
- Is special hard- or software required?
- Does the protection of personal privacy create limitations?
Concrete archiving procedures are developed and applied in implementation of the archiving policy. These archiving procedures translate the general policy into practice, and they are customised to the requirements of the organisation and its records.

Two archiving procedures have been detailed within the DAVID-project: one for office documents and another one for information systems. Both archiving procedures are based upon the general criteria for an archiving procedure and the DAVID-decision model. The electronic classification schema and its electronic files are the focus of attention in the procedure for office documents, while the procedure for information systems departs from the system itself. Tools and instruments were developed during the course of the DAVID-project for implementing both procedures. These tools and instruments were based upon the general criteria for an archiving procedure and the DAVID-decision model. The electronic classification schema and its electronic files are the focus of attention in the procedure for office documents, while the procedure for information systems departs from the system itself.

The following basic principles were applied in developing these archiving procedures:

- Application of the records continuum principle for the electronic records: the archiving procedure starts with the creation or receipt of digital documents, and it continues through to the ingest in the digital repository, their management and dissemination. This means that the archivist becomes involved with records management.
- Integrating as many steps as possible from the "paper world" with which the user is acquainted (registration, filing, etc.).
- Automation of as many actions as possible:
  - Automation enhances the correct application of the archiving procedure with regard to records management.
  - Automation increases user-friendliness.
  - Automation reduces as many steps as possible from the paper world, with which the user is acquainted (registration, filing, etc.).
- The application of the electronic classification schema for the electronic records.
- Application of the electronic archiving standards, etc.

The archiving procedures were applied in developing these archiving procedures:

The implementation of the archiving procedure depends on a number of factors, not least the IT infrastructure in which the procedure is applied. In the first phase, the archiving procedure is applied in the existing IT environment as far as possible. After that, the IT infrastructure in which the procedure is applied evolves. In this way, the users can continue to work in a familiar software environment, and they will become acquainted with the required archiving procedures and archiving management systems. In this way, the users can continue to work in a familiar environment, and they will become acquainted with the required archiving procedures and archiving management systems.
2. OFFICE DOCUMENTS

Actions, such as the creation of electronic files and registration within a digital context, help develop a better understanding of the specific demands that new software will make. This will position one better in defining the functional requirements new software should meet. The development of a classification schema in which electronic files and records are managed is the first step in bringing digital documents under intellectual control.

2.1. DEVELOPING A CLASSIFICATION SCHEMA FOR ELECTRONIC RECORDS

The development of a classification schema is the first step in bringing digital documents under intellectual control. This schema structures the electronic files and organises the electronic records of the organisation. It enables a better understanding of the archival context of the files and the individual items. By basing a classification schema or file plan on the business processes and the functions of the creator, a relationship is established between the files and the business processes in which they were created or received. After all, an archive contains process-related information and its goal is to document business processes. Hence, it is essential that the essential components of the records are determined in a structured way. The business processes and the functions of the creator are primary decision metrics, so that the essential components of the records are brought together in a structured way. The need for a structured and controlled environment for digital documents is crucial.

The DAVID-archiving procedure for office documents consists of six steps:

1. Developing a classification schema
2. Creating and managing quality documents
3. Creating digital files
4. Appraisal and selection for long-term preservation
5. Migration to archiving file formats
6. Ingest into the digital repository and retrieval

The DAVID-archiving procedure for office documents consists of six steps:

1. Developing a classification schema
2. Creating and managing quality documents
3. Creating digital files
4. Appraisal and selection for long-term preservation
5. Migration to archiving file formats
6. Ingest into the digital repository and retrieval
The organisation of records in a classification system is not only important from an archival point of view but also offers a number of practical advantages.

The structure of the archive:

1. Documents are accessible on the basis of consistent descriptions and the structure of the archive, making them easier to find and use.
2. Electronic records can be managed as a group (e.g., appraisal and selection).
3. Creation of files: the link between electronic records and physical records is clear.
4. A record system is established: the logical structure of the archive.
5. The plan of the classification system not only forms the structure in which electronic records are archived, but also delivers important metadata information about the records themselves.
6. In short, a digital classification system is important from an archival point of view.

For a number of reasons:

- Digital documents are created in a structured and controlled environment.
- The bond between the file and the business process on the one hand, and the physical document on the other hand, is documented since the documents are managed within their archival context.
- Digital documents are created in a structured and controlled environment.
- Creation of files: the link between electronic records is established; related electronic records can be managed as a group.
- A classification system makes appraisal possible, so that an excessive preservation of electronic records is avoided.
- The structure of the archive is made visible.
- The classification system makes appraisal of electronic records more accessible.
- A record system is established: the logical structure of the archive.
- Creation of files: the link between electronic records and physical records is clear.
- The bond between the file and the business process on the one hand, and the physical document on the other hand, is documented since the documents are managed within their archival context.
- Digital documents are created in a structured and controlled environment.

In practice, digital classification systems are important from an archival point of view.
Digital archiving

Part 2: Electronic Record Keeping

The same documents will no longer be stored in multiple copies at different
locations: file servers will be unburdened and capacity problems will decrease.
Greater clarity about the value and the importance of documents
is enabled. The system will no longer be overloaded and credit proposals will decline.

Ideally, an electronic classification system is the result of collaboration between
the creator, the IT staff and the archivist. It is advisable to take the time necessary to
develop a joint folder structure, since this structure is the framework within which
electronic records are created and managed. It must be possible for the end-user to
find his way in this structure easily, as otherwise he/she may be discouraged from fil-
ing his records correctly. It is also recommended to foresee a procedure or agree-
ments for the management and control of the classification system, from the moment
that it is defined.

Practical tips and recommendations for the creation of a classification system for
electronic files are available on the DAVID-website:

• Digital Archiving guideline & advice, no. 3: Folder structure and the names

2.2. CREATING AND MANAGING QUALITY DOCUMENTS

To enable a good record keeping system for electronic records, it is important to
create documents of high quality from the beginning. This step is directed towards
the creation and management of authentic, (re)usable and easily archivable electronic
documents. Since the authenticity of an electronic record is linked to its identity and its
accumulator, it is important that the creation and management of the electronic record
take place in a structured and standardized manner. This is the moment to define the
structure of the electronic recordkeeping system, which will be used to manage the
creation and management of electronic documents. The structure of the electronic
recordkeeping system defines the way in which electronic documents are created and
managed. It must be possible to define the organization of the electronic recordkeeping
system in a structured and standardized manner.

This first step is primarily directed towards the organization of electronic files and
records. The specific quality requirements of an electronic record depend on the function
of these records within the business processes in which they are created and
managed.
Digital archiving

Part 2: Electronic Record Keeping

managed. Good records must remain related to the business processes, in which they were created or received (see sections 2.1 and 2.3).

The creation and the management of high-quality records will not only assure that the record keeping procedure proceeds more easily and more efficiently, it will also ensure that more incidental properties of electronic records are saved for the long-term.

2.2.1. The structure

The internal structure of a document is important to structure digital documents internally in an explicit way. Structured documents will survive the ravages of time better and it is easier to process them in another environment. Well-structured electronic documents are more difficult to lose outside of their original software environment. Well-structured documents are also easier to edit and extend. This is one of the standard methods for communicating knowledge in an electronic way. The document model reflects the knowledge that originates after computer data are defined, identified and related. After all, computer data by themselves have no meaning; meaning is attained by defining and clarifying the relationships between the data. The internal structure also indicates how the different components of a document are linked to one another. The more logical relations between the elements of a document are indicated, the better a record will fulfil its function. Success in the migration of a document depends substantially on the structure of its metadata.

2.2.2. The metadata

.successible separately traceable.

The metadata about the document and its context are available. The quality of a record

digital documents can fully fulfill their function as a record in the future, when

The internal structure of a document is not only important because it is useful in the creation and the management of high-quality records, but also because a successful migration was originally created or received (see sections 2.1 and 2.3).
Metadata also depends on the quality of its metadata. Metadata fulfil a variety of functions, such as the identification of the record, supplying information about the archival context of digital documents, helping to guarantee long-term readability, assuring their reliability, etc.

Metadata, exactly like the electronic records themselves, must be permanent, stable and readable. Metadata are stored for at least the same period as the digital documents they relate to. Ideally, metadata of electronic records can be processed automatically.

For metadata a number of quality requirements are applicable, namely:

- fixed
- explicit
- structured
- digital
- readable in the long-term
- linked to a record.

With regard to the metadata of a record, and as a part of the DAVID-decision model, one has to ask oneself what metadata are registered by whom, at what level, and where they will be stored.

Which metadata are necessary depends in part on the type of electronic record and its function.

The metadata about electronic records can be stored in a variety of locations:

- can be encapsulated in a document
- can be stored in a separate computer file
- can be encapsulated in the electronic record (i.e. in the document itself)

Metadata can relate to a variety of different levels:

- the individual record: e.g., the title, author, version, date, a reference to the file folder or the subject matter, a description, keywords, reliability criteria, file name, software, etc.
- the file: e.g., the storage location, ID number, retention period, permanent archival value, (paper) files etc.
- the series: e.g., the storage location, ID number, retention period, permanent archival value, (paper) files, etc.
- the volume: e.g., the storage location, ID number, retention period, permanent archival value, (paper) files, etc.
- the archive: e.g., the creator, the mandate, function, handling, begin-end date, etc.

The metadata of an archived website, for instance, are different from the metadata of an email or a word-processing document. The metadata of a website, for instance, include the publisher, the URL, the author, the date of publication, the title, etc. The metadata of an email, on the other hand, include the sender, the recipient, the date, the subject, etc.

Depending on the type of electronic record and its function, certain types of metadata are more important than others. For example, the metadata of a scientific article might include the title, the authors, the publisher, the date of publication, and the abstract, whereas the metadata of a personal email might include the sender, the recipient, the date, and the subject.

Metadata can be stored in a variety of locations:

- can be encapsulated in the electronic record (i.e. in the document profile/properties, in the file header)
- can be stored in a separate computer file
- can be included in a database.

In practice, a combination of these three possibilities is frequently applied and

...
Digital Archiving

Part 2: Electronic Record Keeping

108

such a decentralised storage has disadvantages regarding automated search procedures. The storage in a centralised database is therefore better, but this does require special care for a persistent link between record and its metadata. Regardless of the storage location, a long-term storage of metadata must also be taken into consideration. Encapsulated metadata, for instance, must be migrated along with the document to the target format (e.g., migration of the document profile of MS Word to XML, TIFF or PDF), and such a procedure may not lead to any readability problems. Databases, in which metadata are stored, are also subject to technological obsolescence.

Wherever possible, metadata are preferably registered in an automated way. After all, many metadata are already present in the computer system. In many cases this requires that the metadata are captured in a static and explicit way and are linked to the document or the file, to which they are related. Another possibility is to compose the metadata automatically. However, not all metadata can be registered automatically. Metadata about the archival context are a typical example of this. These metadata are best registered by those persons who know the contents and functions of the records best, which, in most practical instances, will usually be the administrative staff. If any action is required from the user in this regard, then it is recommended that a very user-friendly solution is provided. Otherwise, the risk that no metadata are assigned is very high.

Metadata are best registered when the document is created or as quickly as possible after its receipt. Since the assignment of metadata is an incremental process, this must be taken into account.

2.2.3. The file format

The choice of the file format in which digital information is stored has direct consequences for the lifespan and the durability of electronic records. If possible, it is highly recommended to store digital documents in a suitable archiving file format from the moment of their creation. This will help to avoid migration and the possible sequences for the persistence and the durability of electronic records. If possible, it is best to choose a format that is less dependent on the manufacturer or the application in which the document was created.

In practice, though, this will not always be possible or desirable. For the purpose of functionality, reusability or user-friendliness, preference can be given to proprietary formats in which documents are created or edited on the computer. In such cases, the migration path (target format, migration tool) must be known at the moment of creation, so that, if necessary, special measures can still be taken during the creation process. Since a record of the creation process is also stored in a database environment, the end-user can select the format and number of other documents that should be included in the record. The format chosen must be known for this purpose.

When a document is saved in a suitable archiving file format, one has to make sure that the applied file format profile is in conformity with the settings that are important from an archival point of view. Most archiving file formats can be extended with special functions that help to preserve the metadata and the content. These functions can be added to the format at the moment of creation.
The reliability of electronic records is assured through a combination of processes and technology. However, the technology of these processes must be replaceable whenever they become outdated. The technological components of these processes, which guarantee the reliability of the long-term preservation of digital documents, cannot be replaced without introduction of new technology. Therefore, the emphasis on the protection of the integrity of the record is often not balanced.

For instance, is not recommended to compose PDF documents with a PDF writer, or to apply JPEG compression when storing a TIFF document. More information on this is available on the DAVID-website:

- F. BOUDREZ, Standaarden voor digitale archiefdocumenten, City Archives of Antwerp, Antwerp, 2002-2005.
- Digital Archiving. guIdeline & aDvice, no. 4: Standards for file formats.

2.2.4. The reliability

There's still no definite answer to the question how long-term reliability can be assured. In any case, the preservation of reliable records is only possible when a procedure that assures such reliability is applied from the moment of creation or receipt of such documents. After all, the reliability must be guaranteed for the entire life-cycle. Such a procedure must, in the first instance, make sure that digital documents cannot be changed without authorisation and that changes are traceable. The emphasis lies on the protection of the integrity of the record. For this purpose, the creator can combine a variety of simple or somewhat more complex measures:

- access control and authorisation: only authorised users have access to files and records (for instance user IDs, passwords, biometrics, PKI)
- 'read-only' access: after archiving or 'capture', the electronic records are fixed and no longer changeable (protected folders and/or files, consultation only)
- version control and maintenance of an audit trail: registration of certain actions on documents is only possible as a new version with a new version number
- access to systems that contain and present the records: only authorised users have access to these systems

These still no definite answer to the question how long-term reliability can be assured in a computerised manner. In any case, the preservation of reliable records is only possible when a procedure that assures such reliability is applied from the moment of creation or receipt of such documents. After all, the reliability must be guaranteed for the entire life-cycle.
Since reliability is an important factor in an appraisal decision, and because of the necessity of demonstrating such a reliability, it is important that the creator documents his reliability procedures, and that these are made available to the archivist.

2.2.5. The user

And finally, the quality of digital documents is also determined through the users: the way in which digital documents are created, metadata are registered and the documents are organised.

The creation of high-quality digital documents depends strongly on the way users compose and save documents. This process can be steered in the right direction by providing the necessary training and through the creation of standard documents or the use of templates. Templates can be used to fix the structure of a document in advance, and perhaps also to anticipate on future migrations of the documents or changes in policy. For example, a template for legal documents could include the following metadata: date and signature of the author, the name of the lawyer, and the number of pages. By providing the necessary training and through the creation of standard documents, this process can be steered in the right direction.

2.2.6. Implementation and examples

The creation of quality digital documents depends strongly on the way users compose and save documents. This process can be steered in the right direction by providing the necessary training and through the creation of standard documents or the use of templates. Templates can be used to fix the structure of a document in advance, and perhaps also to anticipate on future migrations of the documents or changes in policy. For example, a template for legal documents could include the following metadata: date and signature of the author, the name of the lawyer, and the number of pages. By providing the necessary training and through the creation of standard documents, this process can be steered in the right direction.

Two examples of such templates are available on the DAVID-website:

- an e-mail template with a script:
  - automatic registration of metadata: e-mail address of the sender, date and time-stamp of the transmission and receipt, file names of the attachments, the names of the sender and the target folder
  - automatic assignment of a reference code
- a word template with macro:
  - automatic assignment of metadata: insertion of pre-programmed and customised metadata in an automated and user-friendly way

Furthermore, templates also include the possibility of assigning metadata in an automated and user-friendly way. For example, a template could include the following metadata: date and author of the document, the number of pages, and the name of the lawyer. By providing the necessary training and through the creation of standard documents, this process can be steered in the right direction.

The creation of high-quality digital documents depends strongly on the way users compose and save documents. This process can be steered in the right direction by providing the necessary training and through the creation of standard documents or the use of templates. Templates can be used to fix the structure of a document in advance, and perhaps also to anticipate on future migrations of the documents or changes in policy. For example, a template for legal documents could include the following metadata: date and signature of the author, the name of the lawyer, and the number of pages. By providing the necessary training and through the creation of standard documents, this process can be steered in the right direction.
Digital archiving
Part 2: Electronic Record Keeping

Tips and recommendations for good digital documents:
• give office documents a clear identifier (e.g., filename, reference code, etc.)
• define the internal structure of documents in an explicit way; define the structure with the help of (header-) styles, instead of only using text-formatting
• make sure that the content of dynamic fields (for instance an automated date field) is fixed as soon as the document has been completed
• make agreements about the re-use of documents, and for the creation of new versions of an existing document.

2.3 CREATING DIGITAL FILES

Digital files are created and managed in a digital classification system. All digital documents which are created or a task are stored in the same folder. Digital files are created and managed in a digital classification system. All digital documents which are created or a task are stored in the same folder.
The structured classification of electronic records by file or subject folders makes it possible for the administrative staff or archivist to process those digital documents as a group. Appraisal and selection can, for instance, be carried out at a file or subject level. This has, however, consequences, since dropping a document in a certain folder is connected to a decision with regard to its preservation or destruction. Close supervision is recommended in this regard; this is not always easy to achieve.

An essential aspect of the creation of electronic files is the registration of metadata about these files. Important information about electronic files are amongst others: their position within a certain work process, a description, their relation with and the location of a related paper file, the documents in the file, and the retention period. These metadata are common to all documents within the file, and they must be registered in all documents within the file. This is possible with modern document management systems. However, this is not always easy to achieve. Close supervision is recommended in this regard; this is not always easy to achieve.

The structured classification of electronic records by file or subject folders makes it possible for the administrative staff or archivist to process those digital documents as a group. Appraisal and selection can, for instance, be carried out at a file or subject level. This has, however, consequences, since dropping a document in a certain folder is connected to a decision with regard to its preservation or destruction. Close supervision is recommended in this regard; this is not always easy to achieve.

An essential aspect of the creation of electronic files is the registration of metadata about these files. Important information about electronic files are amongst others: their position within a certain work process, a description, their relation with and the location of a related paper file, the documents in the file, and the retention period. These metadata are common to all documents within the file, and they must be registered in all documents within the file. This is possible with modern document management systems. However, this is not always easy to achieve. Close supervision is recommended in this regard; this is not always easy to achieve.
organisation. Digital documents which are not a part of this classification system, effectively escape the archiving procedure and will not be included in the digital repository. One could say that adding a document to a classification system "classifies" the record status of a document.

The classification structure itself and the location of electronic records within this structure are important metadata information. The file/folder structure reflects the context in which the documents are created or managed and indicates the relationship between the documents and within a business process. As a consequence, the folder structure must be archived and should be documented extensively. A loss of the folder structure would, after all, mean a loss of the archival context. It is one of the essential components of a record. A possible solution for this problem is the creation of XML file lists. A hierarchical overview of the folders is created in such a file list, including a mention of the documents that are stored in those folders.

2.4. APPRAISAL AND SELECTION FOR LONG-TERM PRESERVATION

The issues regarding appraisal and selection are situated at two different levels within the digital world: the file and the records. At file level, the question regarding selection focuses above all on which files are preserved and which are destroyed. At record level, based on appraisal, a decision is made as to which components are essential and which are incidental. In case of paper documents, this last question does not pose itself because the entire paper record is preserved.

The records schedules for paper files are equally valid for electronic files. No other retention periods apply for electronic files. Brought into practice this means that at a given point in time, those files, which are considered for long-term archiving, are selected and removed from the active classification structure. Such a selection can be carried out on the basis of a manual and/or automatic selection procedure. The latter method, however, requires that the retention period is indicated and processeable in one way or another. One possibility is, for instance, to include the retention period and the disposition in the metadata of the file.

For appraisal and selection, it is not an unnecessary luxury to register metadata at file level. These metadata provide information about the context and the value which the creator assigns to the files in the electronic classification system. The fact that administrative staff members have assigned retention periods does not replace the need for retention schedules. Quite the contrary, the assignment of a retention period on the basis of manual or automatic selection procedures is mainly based on appraisal, a decision is made as to which components are essential and which are incidental in case of paper documents. A historical overview of the folders is created in such a file list including a mention of the documents that are stored in those folders.

At document level, the problem concerning appraisal and selection is actually continuously present in the archiving procedure. The components of the document are essential and must therefore be archived. The same question arises again before deciding on a migration path to a suitable repository.
part 2: electronic record keeping

114

2.5. MIGRATION TO ARCHIVING FILE FORMATS

After selection and before digital documents are included in a digital archive, they must, if necessary, be migrated into a suitable archiving file format. This offers two advantages:

- Firstly, only electronic records with permanent archival value are migrated, which saves costs and time.
- Secondly, the migration can occur under the responsibility of the creator, who can declare migrated documents as authentic.

Those electronic records, which are stored in an archiving file format from the moment that they are created, need not be migrated. It is recommended to check whether the correct settings from an archival point of view were used, if necessary.

After migration, the system that is used for the migration should provide the following functionalities:

- Successfully migrated, so that these can subsequently be migrated manually.
- Error-free and error-free migration: extensive testing.
- The possibility of configuring which profile of the archiving file format to apply.
- 100% correct application of the form of standard or specification.

Migration to a suitable archiving file format is preferably performed with reliable migration tools, which can be purchased or developed. Special requirements are therefore applicable to migration tools:

- 100% correct application of the file format standard or specification.
- The possibility of configuring which profile of the archiving file format to apply.
- Error-detecting and reporting: registration of which documents were not migrated correctly.
- Available and controllable source code: migration software can be developed, both commercial or open source tools can be used for the migration, existing applications can be customized, or custom software can be developed.

Migrating electronic records into a suitable archiving file format is an important step in ensuring the long-term survival of digital documents. It is crucial to select the right format and to perform the migration correctly to ensure that the records remain accessible and usable in the future.
2.6. Ingest into the Digital Repository and Retrieval

2.6.1. Verification and Registration

On receipt in the archival service, the transferred documents must be verified and registered.

2.6.2. Searching for Archived Files and Records

The user can be given access to the archived electronic records on a variety of different levels:

- The creator of the transferred records, whenever these are also served as the new acquisitions.
- Computer viruses.
- Faulty storage media.
- The presence of instruments for record retrieval:
  - The completeness of the transfer: does the storage media contain all records (for instance, a check on the basis of an XML file list, which has been used to establish the list of the records that have been provided with metadata).
  - The completeness of the transferred records: does the conversion process produce all the metadata that can be derived from the original bitstream.
  - The completeness of the transfer storage media: does the transfer storage media contain all records.
  - Computer viruses.

For instance, a check on the basis of an XML file list, which has been used as a transfer list:

- The completeness of the transferred records: does the transfer storage media contain all records.
- The creator of the transferred records, whenever these are also served as the new acquisitions.
- Computer viruses.
- Faulty storage media.
- The presence of instruments for record retrieval:
  - The completeness of the transfer: does the storage media contain all records (for instance, a check on the basis of an XML file list, which has been used to establish the list of the records that have been provided with metadata).
  - The completeness of the transferred records: does the conversion process produce all the metadata that can be derived from the original bitstream.
  - The completeness of the transfer storage media: does the transfer storage media contain all records.
  - Computer viruses.

Whenever during such a verification problems are detected or the predefined quality requirements are not observed, the creator must be contacted and asked to resolve the problems. After a positive evaluation of the quality, the creator is given permission to delete the documents and the new acquisitions are registered. Then an inventory of the records is prepared and their metadata are completed. In this regard, attention must be given to the unique ID number for each of the electronic records. During registration, the user can be given access to the archived electronic records on a variety of different levels:

- The user can be given access to the archived electronic records on a variety of different levels:
- The creator of the transferred records, whenever these are also served as the new acquisitions.
- Computer viruses.
- Faulty storage media.
- The presence of instruments for record retrieval:
  - The completeness of the transfer: does the storage media contain all records (for instance, a check on the basis of an XML file list, which has been used to establish the list of the records that have been provided with metadata).
  - The completeness of the transferred records: does the conversion process produce all the metadata that can be derived from the original bitstream.
  - The completeness of the transfer storage media: does the transfer storage media contain all records.
  - Computer viruses.

For instance, a check on the basis of an XML file list, which has been used as a transfer list:

- The completeness of the transferred records: does the transfer storage media contain all records.
- The creator of the transferred records, whenever these are also served as the new acquisitions.
- Computer viruses.
- Faulty storage media.
- The presence of instruments for record retrieval:
  - The completeness of the transfer: does the storage media contain all records (for instance, a check on the basis of an XML file list, which has been used to establish the list of the records that have been provided with metadata).
  - The completeness of the transferred records: does the conversion process produce all the metadata that can be derived from the original bitstream.
  - The completeness of the transfer storage media: does the transfer storage media contain all records.
  - Computer viruses.
Giving access at record level depends also on the availability of metadata for each record. In order to give access at the record level, this means that the metadata of each digital file must be known and can be processed. If these metadata have been stored in a digital, explicit and structured way, they can be included in the database automatically.

In order to give access at the file level, this means that the metadata of each digital file must be known and can be processed. If these metadata have been stored in a digital, explicit and structured way, they can be included in the database automatically.

The level and the way in which digital files and records are queried depend on the availability of metadata for each digital file.

Two methods are provided for this:

1. The storage of metadata in a database

   - This allows for more detailed searches and records to be retrieved more quickly.
   - Giving access only at a series level (type) level, such as for instance "personnel files," is too general to allow efficient retrieval of these files.

2. The file level

   - Giving access at the file level allows for more targeted searches.
   - Searching at the record level allows for more targeted searches.

We will discuss how records can be searched for both levels below.
Searching for files and records is also possible on the basis of XML file lists, which were created as documentation of the electronic classification system, and which were also used as a transfer list (see item 2.3 and 2.6.1). This method does not make use of a database, in which all the files and/or document metadata have been stored. Instead, the XML file lists are used to search within a certain folder. When accessing the archives on the basis of an XML file list, the search path remains largely limited to the structure of the archive which is based on the business processes and activities. The archived files and records must be made accessible in a more explicit way for external users of the archives. The search procedure is then based on the file names of the records, which are included in the XML file lists. If required, they can be displayed under the folder names in the interface with the search results. Also the file type can be a guideline during a search procedure. Since the search procedure is now already refined to searching within a certain folder, an "on-the-fly" query of the content of the documents can proceed more quickly and in a more targeted way. However, in the search path, the documents must be searched one by one, which can be time-consuming for large quantities of documents.

Searching records is a two-step process in this case. The user first searches for the relevant files, by browsing through the business processes, tasks and activities of the records creator. Subsequently, the desired document is searched for within the located folder. Such a search procedure proceeds primarily on the basis of the file name of the document. Since the file names of the records have been included in the XML file lists, they can also be displayed under the folder names in the interface with the search results. However, this is less suitable for external users of the archives. The archived files and records must be made accessible in a more explicit way for them. XML topic maps could be a solution for this need. On the basis of a topic map, external users can retrieve archived files and records, based on their own associations and search paths. The XML file lists can be used as building blocks for an XML topic map.

More information on this is available on the DAVID-website:

3. INFORMATION SYSTEMS

3.1. CHARACTERISTICS

Besides digital office documents, organisations maintain large-volume information systems. These systems have a number of special characteristics which make a separate archiving procedure necessary for each of them. These characteristics include the following:

- The information systems are usually managed centrally on mainframes and servers, and they cannot be handled by creating files.
- The documents are integrated within the user interface of the information system, which is accessible through a number of different channels. They are not stored in a document-oriented way but rather as part of an integrated whole of interactive applications.
- The data which is created and managed in these systems does not always have a fixed documentary form. This is due to new technologies and the fact that documents are not used as their basis.
- The documents are usually re-composed at the moment that they are requested, and they are not statically stored as a single document. The content of the documents depends on the information which is available at the moment of interaction with the user.
- The data/document system is integrated with databases, which in turn are part of a larger information system.

As a consequence of these characteristics, the archiving of information systems also includes the following:

- The capture (identification, storage and registration) of records is an essential part of the archiving procedure for information systems. The records are identified in these data-centric information systems on the basis of appraisal.
- The dynamic and interactive character of these information systems makes this self-evident.
- The basis of appraisal is the dynamic and interactive character of these information systems, while the records are identified in these data-centric information systems on the basis of appraisal.

Electronic records are an essential part of the archiving procedure for information systems. The capture of records is an essential part of the archiving procedure for information systems. The records are identified in these data-centric information systems on the basis of appraisal. The dynamic and interactive character of these information systems makes this self-evident.
3.2. THE INFORMATION SYSTEM AS STARTING POINT

The starting point for an archiving procedure is the information system, in which the documents are created and managed. To define the actual creation of the documents themselves, which are created and managed, the archiving procedure starts with the design and the development of the information system. The first steps in the archiving procedure are taken at a very early stage. The archiving procedure starts with the creation up to the ingest into the digital repository and giving access. Just as with office documents, the archiving procedure for information systems is in most cases the system administration, but there are possible exceptions. The answer to the question of what the documents need to be archived HOW and WHERE is not only dependent on the information system itself but also on the documents that need to be archived. The archiving procedure must be tailored to the characteristics of the documents, particularly the metadata, the dependencies, the interactions, etc. Each information system should be analyzed to find out its specific needs. The starting point for an archiving procedure is the information system, in which the documents are created and managed.
The procedure starts with informing the archivist and the registration of metadata about the information system. The creator informs the archivist about the development of the new information system, the adaptations to an existing information system or the dismantling of an outdated information system. It is best to include this notification obligation within the organisation as a formal step in the general IT procedures. Preferably, such a notification should be done as early as possible so that the archivist has enough time for an analysis and anticipative measures, and does not lag behind the facts. The aim of this step is informing the archivist so he knows for what type of information system an archiving solution is required, so that he will be involved in the development, the adaptation or the dismantling of the corresponding information system.

Since the archivist requires information about the information system for planning his following steps in the archiving procedure, it is important that documentation about the information system is provided for registration and maintenance as early as possible, and in a structured and organised way. Metadata about information systems are, however, not systematically maintained in most administrations or IT departments. As a consequence, archivists only dispose of the information system itself at the moment of archiving, in the best of cases including some verbally provided information about the system. It speaks for itself that this is an insufficient basis for important decisions, such as the identification of records, appraisal and the development of an archiving strategy.

The metadata about information systems are registered and maintained in a new archiving instrument: an information systems inventory. From the day of its creation, metadata about the electronic information system are maintained in this inventory by the creator, the system administrator(s) and the archivist. The basic data model for this management inventory are the data fields that are required from an archival point of view. These refer to the creation context, the technical context and the management context. Such an information systems inventory can, however, also serve other goals, concerning, e.g., a helpdesk function or the management of the IT infrastructure. In this way, the creation of the system administrator(s) and the archivist function as the basic data model for this inventory.

The metadata about information systems are registered and maintained in a new archiving instrument: an information systems inventory. From the day of its creation, documentation about the electronic information system is maintained in this inventory by the creator, the system administrator(s) and the archivist. This inventory offers an added value for the entire organisation, whereby the creator and the archivist are not the only interested parties for keeping the inventory up-to-date. An information systems inventory can, however, also serve other goals, concerning, e.g., a helpdesk function or the management of the IT infrastructure. In this way, the creation of the system administrator(s) and the archivist function as the basic data model for this inventory.
In order to answer the WHAT question it may be useful to view the information in the future. According to what criteria do the archivist examine the technical requirements for faithfully reconstructing the records? The choice depends also on the technical requirements for faithfully reconstructing the database itself, whether or not additional data is needed, and whether the database is a record or an aggregation of records. The archivist will also examine whether a particular output from the database is a record or not.

During the process of identifying the records, the archivist must also define the boundaries of the record. Many information systems are linked to each other and draw information from external sources. On the basis of the identification of the records and appraisal, the archivist determines whether the external information is archived as a part of the information system.

Records with a limited retention period, or those where the lifespan is limited to that of the information system itself, can probably be preserved within the active information system, whereas a long-term solution must be provided outside the information system. If records are created and managed within the information system, then the records are captured as conceptual objects, so an interpretation is possible in the future. The archivist will answer the WHAT and WHEN questions immediately to a retention period for the records, and also to the question of whether the records are created as part of the acquisition of the information system. The archivist will also answer the WHAT and WHEN questions immediately to a retention period for the records.

If no records are created within the information system, then special requirements are defined for the information system. No archiving procedures are developed and no existing procedures are developed, and also the format of an archival point of view no information system is an important source. These processes in the case of adaptations or dismantling of existing systems.
These three layers can be linked to the five components of the record. An identification of the essential and the incidental components of the record will determine which layers or which parts of that information system are archived. In this way a differentiation is, for instance, made in the data layer, between computer data and records, whenever the database is not the complete document itself. The records are collected by a query, which is created on the basis of appraisal. The result of this query will subsequently be exported from the database system and archived. When, by contrast, the database itself is the record, then substantial attention must be paid to the structure. The parent-child relationship is important for hierarchical databases, whereas the relationship between the tables and the structure of the records must be archived together with relational databases. The context of a record is somewhat of an exception in this case, since the context and the metadata of the information system are documented in the information system inventory. Since the context and the metadata of the information system are documented in the information system inventory, both can be distilling from this inventory. For those records, which are taken into consideration for long-term archiving, it is recommended to define WHEN they will be removed from the information system. An answer to the WHEN question can depend on a number of different factors:

- limitations of the storage system
- performance level of the computer system
- replacement or upgrade through a new information system
- support by suppliers
- acquisition and development costs
- exchangeability, plug-ins, etc.
Regardless of the retention period, and on the basis of the WHAT and WHEN questions, this step examines whether there are special requirements that apply to the information system, with regard to the creation, maintenance and an efficient archiving of good electronic records. These requirements can refer to such items as:

- the encoding of data: application of standards, storage of documentation
- the file format in which the documents are stored and the quality requirements
- the registration of metadata
- the archiving of changes, or the creation of a version history
- the registration of documentation
- the integration of reliability guarantees and measures
- the provision of an archiving module, so that documents can be archived in a simple and automated way.

The transient and interactive character of information systems is frequently in conflict with the stable characteristics that are required of records. The data in databases are continuously augmented or changed, while records, per definition, take a fixed documentary form with a permanent content. Because of the necessity for reconstructing data, it is frequently recommended to maintain a history of the data and their changes. Such a history can be maintained either within the database itself or by logging in a separate log file. The main reason for keeping a history is that it can be used for auditing and for proving that data have been changed. This makes the log a central part of the archival process.

The standard log files contain much more information than just the data that have been changed. They also save the who, when, and why of the changes. This means that the use of standard log files is not very practical for archival purposes. A better solution is to create a separate log for archiving and to define in advance which actions are to be logged in the log file. This log file should be kept outside of the database and can be converted to an archiving file format at a later date.

The following are the main features of a suitable archiving file format:

- It should be easy to convert the data from the database to the archiving file format.
- It should be possible to read and interpret the data in the archiving file format.
- It should be possible to maintain a history of the changes that have been made to the data.
- It should be possible to perform searches on the data in the archiving file format.
- It should be possible to access the data in an efficient manner.

The standard file formats that are used for archiving are typically defined in a formal way. This means that a format profile and its ideal archiving settings are defined in advance. In the absence of a suitable archiving file format, the records can be stored in an exchange format. If no other solution is available, then storage in the application-dependent format is a practical solution.
files. XML, together with ASCII or Unicode, is the recommended archiving file format for purely textual databases. Binary objects that are stored in a database, or the generated output of such data, are best converted to the archiving file format that is most closely linked to their type.

In most cases, it is advisable to define the archiving file format at the time that the archiving procedure is developed. This is not always possible in practice, in which case it is better to wait and see what options are available at the time that one proceeds to archive. Information technology and standardization are, after all, continuously developing.

The next part of the question is the HOW aspect of the decision model, concerning the preservation medium that is used for transmission and/or long-term storage. The archival service determines which media are used for transferring data. In principle, every type of storage medium can be taken into consideration, which can be read by the archiving service. However, it is not self-evident when large quantities of computer files must be transmitted. The archival service transfers these files to a suitable long-term storage medium.

The records are registered and made accessible when the transferred data do not successfully pass the quality checks. In this case, matters become somewhat more complex, when the archival service also wants to use the transfer medium as the long-term storage medium. Strict quality requirements, for writing data to and manipulating it on these storage media, apply.

More information on this is available on the DAVID-website:

- F. BOUDREZ, The digital recordkeeping system: inventory, information layers and a decision-making model as a point of departure. City Archives of Antwerp, Antwerp, 2001 (DAVID report no. 4).
- F. BOUDREZ, From electronic records to database-driven information management. A decision-making model as a point of departure. City Archives of Antwerp, Antwerp, 2001 (DAVID report no. 4).

More information on this is available on the DAVID-website:

- F. BOUDREZ, The digital recordkeeping system: inventory, information layers and a decision-making model as a point of departure. City Archives of Antwerp, Antwerp, 2001 (DAVID report no. 4).
- F. BOUDREZ, From electronic records to database-driven information management. A decision-making model as a point of departure. City Archives of Antwerp, Antwerp, 2001 (DAVID report no. 4).
Digital archiving offers several challenges, but also a long way off. However, this does not mean that technological solutions aren’t important parts of the procedure will be different for every organisation.

Archival science must provide the leading guidance in tackling the problems involved with the long-term preservation of electronic records. Especially the identification of the records and their appraisal are the keystones for every record keeping system. Identifying the long-term preservation of electronic records, especially the records involved with the long-term preservation of electronic records, must be done before there are no solutions at the box for electronic records keep.

E. Conclusion

• Preservation of websites
• Population register
• Electoral register
• DAVID-cases:
  • F. BOUDREZ, Presentation of electronic records from databases driven information systems. EPrints, City Archives of Antwerp. 2003.
giving access to the preserved records. At the moment, the technological solutions to solve a wide range of obstacles are available today and are ready to implement.

In any case, it's recommendable to start the record keeping procedure before the actual electronic records are created. This is the only way to apply an effective record keeping system. By doing so, one can also save on the investment of time and resources. Retro-active archiving initiatives will never have the same result as the usual electronic records are created. This is the only way to apply an effective record keeping strategy for the electronic records and their metadata.

When choosing tools and instruments, one has to make sure that these are suited with the organisation's overall procedure and more particular with its digital workflow. This means that choosing tools and instruments one has to make sure that these are able to solve a wide range of obstacles and are ready to implement.
Part 1: The Legal Framework for Business Archives


2. Article 355 and following of the Civil Code.


4. Article 1315 and following of the Civil Code.

5. Contrary to the rules of evidence in tax matters and in criminal cases where, in principle, every type of evidence is admissible and the court judges its credibility.

6. The concept “evidential value” relates to the faith that the court places in evidence. It is only when the court has assigned evidential value to an piece of evidence that one can speak of proof. In principle, it is the court that judges the evidential value of the evidence submitted to it. For some pieces of evidence, such as the signed document, the law determines the evidential value.

7. The law did not define the concept signature before the electronic signature was introduced. This definition was developed in jurisprudence and in doctrine.


9. The problem resides in the value of electronic documents as evidence. There is no difficulty now (nor was there in the past) with the validity of agreements reached electronically. There are no special formal requirements, such as handwriting, to prove the authenticity or validity of a contract reached electronically. There are no special formal requirements, such as handwriting, to prove the authenticity or validity of a contract reached electronically. There are no special formal requirements, such as handwriting, to prove the authenticity or validity of a contract reached electronically.
Part I: The Legal Framework for Business Archives

Companies carrying out activities of a special nature that require a specific form of financial statement (such as credit institutions, insurance companies and holding companies) are required to submit their statements in paper form. The size of a company is considered large depends on whether or not it has exceeded the size criteria described in Art. 15 of the Corporation Law Code.

For VAT, since 1 January 1993; for income tax, since 16 July 1994.

Cf. above: the central ledger, the integral journal, the three journals and the inventory ledger.


For WORM (write once, read many) storage devices, such as a CD-ROM or WORM diskette, these media guarantee that entries will not be modified or reversed in the same way as paper does, if not better. Software can also be designed in such a way as to make changes impossible.

Article 6 of the Accounting Act.

Article 14 §2 of Royal Decree no 1 of 29 December 1992.

Art. 1 §2 of Royal Decree no 1 of 29 December 1992.

Cf. above.

Study on the Requirements Imposed by the Member States, for the Purpose of Charging Taxes, for Invoices Produced by Electronic Means, PricewaterhouseCoopers, Final Report, 23 August 1999.

This involves administrative co-operation agreements of similar tenor to Directives 76/308/EEC and 77/799/EEC and (EEC) Ordinance of 7 December 1988 on the income tax reform and changes to taxes equivalent to stamp taxes stipulates that micro cards or microfilms of the registers have the same evidentiary value as the originals when they have been prepared by or at the behest of the income tax authorities.


Law of 17 July 1975 on company accounts.


Cf. above.


This means that a consensus on this matter must be reached in a plenary session of the Council of Ministers, in contrast to a normal royal decree, what can be enacted by just one minister.


Moniteur belge, 29 September 1979 (L 15/24, 17.1.2002).

Part I: The Legal Framework for Business Archives

1. Digital Archiving

2. The Telematics Commission, “Langetermijnbewaring van patiëntendossiers in ziekenhuizen.”


6. The legislator makes no distinction between an electronically or manually maintained medical file.


15. Law of 26 July 1996 on the modernization of the social security system and protection of the maintainability of the legal pension systems.

16. Art. 4 §4 of Royal Decree no 5 of 23 October 1978 on maintaining social documents.


20. Art. 4-10 of the Royal Decree of 8 August 1980 on maintaining social documents.


28. Art. 6 of the Royal Decree of 23 October 1978 on maintaining social documents.


32. Royal Decree of 17 June 1994 on keeping an attendance register.

33. Royal Decree of 18 February 1983 establishing the modalities for maintaining and preserving social documents for recognized dockworkers.


35. Royal Decree of 1 November 1990 on the checking and checking of the documentation concerning the duration of employment in the diamond industry.


37. Royal Decree of 30 November 1983 establishing the rules for maintaining and storing an attendance register in the diamond industry.

38. Royal Decree on maintaining an attendance register in the hospitality industry.

39. Royal Decree of 22 November 1990 on the checking of the documentation concerning the duration of employment of dockworkers.


42. Royal Decree of 30 December 1989.


44. Royal Decree of 1 November 1990 on the checking and checking of the documentation concerning the duration of employment in the diamond industry.


46. Royal Decree of 30 November 1983 establishing the rules for maintaining and storing an attendance register in the diamond industry.

47. Royal Decree on maintaining an attendance register in the hospitality industry.


Art. 7 §2 j) of the Privacy Act.

Art. 10 of the Patients’ Rights Act.


Art. 3bis 1° Privacy Act.

Art. 1 §4 of the Privacy Act.

Art. 1 §5 of the Privacy Act.

Art. 1 §1 of the Privacy Act.

Art. 1 §2 of the Privacy Act.

Art. 3 §1 of the Privacy Act.

These include the Belgian State Security Service, the Belgian Military Intelligence Service, Belgian National Security Authority as well as the security officers, the Permanent Supervisory Committee and the Investigatory Department of the Belgian Intelligence Service, insofar as the processing is required in the exercise of their assignments.

Art. 3 §§4-7 of the Privacy Act.

Art. 5 a of the Privacy Act.

Art. 5 b of the Privacy Act.

Art. 5 c of the Privacy Act.

Art. 5 f of the Privacy Act.

Art. 4 §1 2° of the Privacy Act.


Art. 4 §1 3° of the Privacy Act.

Art. 4 §1 4° of the Privacy Act.

Art. 4 §1 5° of the Privacy Act.

Art. 9 §1 of the Privacy Act.

Art. 9 §1 par. 1 and §2 par. 1 of the Privacy Act.

This refers specifically to a law, decree, ordinance, royal decree or a ministerial order.

Art. 9 §2 par. 2 b) of the Privacy Act.

Art. 9 §2 par. 2 a) of the Privacy Act.

Art. 30 of the Privacy Decree.

Art. 10 §1 a) of the Privacy Act.

Art. 10 §1 b) of the Privacy Act.


Art. 10 of the Privacy Act and art. 32 of the Privacy Decree.

Art. 3 of the Privacy Act.

Art. 13 of the Privacy Act.

Art. 12 §1 par. 1 and 5 of the Privacy Act.


Art. 12 of the Privacy Act and art. 32-33 of the Privacy Decree.

Art. 3 of the Privacy Act.
Art. 25-27 of the Privacy Decree.
Art. 6 §1 of the Privacy Act.
Art. 6 §2 of the Privacy Act.
Art. 6 §2 1) of the Privacy Act.
Art. 7 §1 of the Privacy Act.
Art. 7 §2 of the Privacy Act.
Art. 7 §2 e) of the Privacy Act.
Art. 7 §4 of the Privacy Act.
Art. 7 §5 of the Privacy Act.
Art. 10 §2 of the Privacy Act.
Art. 8 §1 of the Privacy Act.
Art. 8 §2 of the Privacy Act.
Art. 8 §2 b) of the Privacy Act.
Chapter II of the Privacy Decree.
Art. 17 of the Privacy Act.
Art. 17 §8 of the Privacy Act.
Art. 51-62 of the Privacy Decree.
Art. 31bis of the Privacy Act.
Art. 36bis of the Privacy Act.
Art. 16 §1 of the Privacy Act.
Art. 16 §2 of the Privacy Act.
Art. 16 §1 of the Privacy Act.
Art. 21-22 of the Privacy Act.
Art. 22 a1. 1 of the Privacy Act.
Art. 22 a1. 2 of the Privacy Act.
Art. 41 of the Privacy Act.
Art. 29 Constitution.
Art. 259bis and 314bis of the Belgian Criminal Code.
“Knowingly and willingly” is a term used in criminal law. It means that the person committing the crime was aware of the fact that he was committing a crime (the maxim “everyone is presupposed to know the law” plays a role here) and that, knowing quite well what he does, he wants to commit the offence.
HENDRICKX, F., *op. cit.*, 190 and 195.
Art. 109terE 1° of the Telecommunications Act.
Collective Labor Agreement no 81 of 26 April 2002 on the supervision of the use of internet and e-mail at work and the protection of employees’ personal privacy, declared binding by the Royal Decree of 12 June 2002 (*Moniteur belge* 29 June 2002).
For a general discussion on this topic, see HANNELORE DEKEYSER, “C.A.O. nr. 81 tot Bescherming van de Persoonlijke Levenssfeer ten opzichte van de Controle op de Elektronische On-linecommunicatiegegevens” in *X.*, *Mediarecht*, Brussels, Kluwer, loose leaf.
For instance, time sent, sender, addressee(s), attachments, and reference to an answer to the message.
Art. 9 of CLA no 81.
Part 1: The Legal Framework for Business Archives

197 A more sophisticated method consists in adding an extra field to each e-mail in which the employee must enter a file number or a classification code. This information immediately situates the e-mail in its context.

198 Art. 16 of CLA no 81.


202 Art. 3 §1 and 2 of the Copyright Act.

203 Art. 3 §3 of the Copyright Act.

204 Art. 80, par 1 and 2 of the Copyright Act.


206 Art. 80, par 4 of the Copyright Act.

207 Fines must always be multiplied by a factor to take inflation into account. The conversion of fines into euros was regulated in the law of 26 June 2000 (Moniteur belge 29 July 2000). See: http://www.just.fgov.be The Judiciary and the Euro.

208 Art. 1481ff of the Judicial Code.

209 Art. 587 par 1, no 7 of the Judicial Code and art. 87, §1 of the Copyright Act.

210 Art. 87 §2 of the Copyright Act.

211 COM (88) 816 final, O.J. C. 12 April 1989, no 91, 9.

212 Art. 10 of the Software (Protection) Act.

213 Fines must always be multiplied by a factor to take inflation into account. The conversion of fines into euros was regulated in the law of 26 June 2000 (Moniteur belge 29 July 2000). See also: http://www.just.fgov.be The Judiciary and the Euro.


216 A producer is established in the EU when he/she is a citizen of a member State or has his/her normal residence in a Member State. A company is established in the EU when the company is established according to the legislation of a member State and when the registered office, the central administration or the main establishment is located in the Union. If the company only has its registered office within the territory of the Union, its activities must have an essential and durable bond with the economy of a Member State.

Art. 12 of the Database Protection Act.

217 Art. 3, par. 1 of the Database Protection Act.

218 Art. 2, 2 of the Database Protection Act.

219 Art. 2, 3 of the Database Protection Act.

220 One example is when one would provide access to information from someone else’s database on one’s own portal site. The users of the portal site would only request a limited amount of data from the database (non-substantial part). Yet this harms the producer’s legitimate interests because users do not visit his/her site directly and see the advertising there.

221 Art. 13 of the Database Protection Act.

222 Art. 14 of the Database Protection Act.

223 Art. 15 of the Database Protection Act.

224 See above.


226 www.creativecommons.org.


228 This is also called Public Key Cryptography (as opposed to Private Key Cryptography), because it uses one key that is known to everyone and hence is public.

REFERENCES PART 2