Représentant les avocats d'Europe
Representing Europe's lawyers

ELECTRONIC COMMUNICATION AND THE INTERNET

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.org – www.ccbe.org

Summary of guidance

I. Content of e-mail and Internet sites

1. Data

- Keep it accurate and updated
- Comply with professional rules (a basic requirement is usually the name and address of the firm as well as the name of its partners or a statement about where this information can be obtained)

2. Nature of the on-line legal service

- Explain the nature of the legal advice being provided so as to avoid misunderstandings and possible claims against lawyers for inaccurate or incorrect advice

3. Links and references to third parties

- Care must be taken to ensure that these sites do not appear offensive to the profession, or incompatible with the profession's underlying principles

II. Lawyer correspondence

1. Deliberate interception and hacking

- Use appropriate means for electronic signature to protect the content of correspondence against any fraudulent modification
- Use means of electronic communication which are reasonably protected against any interception and hacking which could result in the disclosure of existence and content of communication
- Use encryption techniques which are reasonably available every time clients or correspondents request them
- Inform clients and correspondents, if necessary, of the risks encountered by the use of electronic communications

2. Inadvertent access

- Include automated confidentiality warnings

3. Viruses and malicious software

- Develop a security strategy and basic security procedures

4. Electronic mail correspondence between lawyers

- Bear in mind the professional rules applicable to correspondence between lawyers when using e-mails

III. Safeguarding personal data: data protection legislation

- Sending, receiving and holding e-mail correspondence may involve the processing of personal data which must be dealt with in accordance with data protection legislation
- Display a data protection notice

IV. Safeguarding copyright

- Verify copyright protection and use copyright notices if required by legislation

V. Best practice

- Verify the identity of an on-line client
- Give a timely response to an on-line client
- Keep records of electronic correspondence
- Maintain user privacy and monitor standards for electronic correspondence
- Comply with professional rules regarding on-line cross-border disputes

VI. Archiving of electronic documents and e-mails

- Develop fixed policies regarding the archiving of electronic documents and e-mails, not only on what should be archived, but how it should be archived, in order to preserve accessibility to the electronic documents and e-mails in the future
- Be aware that saving electronic documents and e-mails in one program might have consequences for the possibility to retrieve them in the future
- Archive electronic documents and e-mails using a generally accepted format, ensuring their legibility in the future, and the safeguarding of the original version

ELECTRONIC COMMUNICATION AND THE INTERNET

Guidance for Lawyers

CCBE

FOREWORD

1. The electronic provision of legal services, via electronic mail ("e-mail"), the Internet or any other new technology, offers lawyers an opportunity to enhance the quality of their services and the speed at which these can be delivered to their clients. Without proper guidance, however, e-services can result in serious losses for which a firm, and lawyer, may be held liable.

2. As a communication tool, e-mail is easy to use and many users tend to regard it as if it were a spoken medium rather than a written one. As a result, the content of some e-mails may well be regarded as defamatory or offensive if it is read by an unintended recipient. Both the lawyer sending the message, and the firm employing him/her, may be held liable.

3. Internet sites (or websites) are increasingly being used by law firms as advertising tools but also as a means of disseminating legal advice and information. Many lawyers feel that providing legal services on-line offers the opportunity to access a much wider client base, to decrease overheads (the lawyer no longer needs an office), to have flexible working hours and to streamline case work procedures by downloading Internet tools such as case-management software. But the Internet also presents clear dangers for lawyers. The absence of a face to face meeting with a client, could make it more difficult for a lawyer to assess a case and to provide complete advice, an on-line client could usurp the identity of another person (for a will, for example), a person could wrongly portray him/herself as a lawyer.

4. The archiving of electronic documents and e-mails will be an issue of greater importance in the near future. The CCBE therefore thought it necessary to make the national Bars and Law Societies aware of the fact that both digital and paper records must meet the same legal requirements when sent and archived. It recommends the adoption of policies regarding the archiving of electronic documents and e-mails.

5. To reap the benefits of on-line technology while minimising its dangers, firms need to consider how legal professional standards and best practice can be translated into the electronic world. The CCBE believes the most effective way to do this is by drafting an Internet and electronic mail policy.

6. To assist law societies, bars and firms in producing their own policy, the CCBE has drafted a model Internet and e-mail policy. This may need to be adapted to a country's own professional rules and to the firm's particular circumstances. It is recommended that, once adopted, the policy be disseminated among all the firm's staff together with other conduct advice.

I. Content of e-mail and Internet sites

A lawyer and firm's liability for wrong or misleading information can be engaged when providing advice or information electronically or on paper. Care must therefore be taken to check that data is accurate, updated and in compliance with professional rules.

1. Data: Complying with Professional Rules

a) Principles:

The information required in lawyer correspondence may vary from country to country. Generally, all professional rules require basic information which will allow a client to verify the firm's credentials and file a complaint against the firm. The latter will comprise: the name of the firm, its address, the name of the firm's partners, or, a statement about where this information can be obtained, and any other information on the registration of the service provider in accordance with the EU Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)[1].

b) Guidance:

For Internet sites, law firms are advised to provide this information in a clearly visible notice on the home page.

For electronic mail correspondence, law firms may wish to introduce templates, as described below.

E-mail software can provide its users with one or more standard templates incorporating the information they must provide in their correspondence.

When firms permit users to send private e-mail, they are recommended either to ask solicitors to write private e-mails on an alternative template that expressly states that the communication is from the user alone and not the firm or to require that lawyers apply a different signature block for private communications.

When firms permit users to take part by e-mail in public discussions on mailing lists, confidentiality or privilege warnings are obviously inappropriate, and their inclusion can detract from the impact of the message. Firms may wish to consider adopting a specific template for such purposes.

2. Nature of an on-line legal service

a) Principles

Many of those who contact a law firm through its website or via e-mail have little or no legal knowledge. In order not to mislead the client, it is therefore imperative that the lawyer clearly explain when his/her communication constitutes legal information and when it constitutes advice.

Generally, "information" can be defined as material which will be the same, irrespective of the person requesting the legal service. If, on the other hand, material will depend on the person requesting the service, then the service can be defined as "advice".[2]

b) Guidance:

In e-mail correspondence, the lawyer will need to clarify when information provided constitutes legal advice and when it is only information. The context of the e-mail correspondence can assist in establishing the nature of the service.

For Internet sites, firms are advised to state clearly on the home page that the services provided by the site are for information only. Without minimal contact, it is impossible for a firm to offer advice, which is why many sites will state that legal advice can be obtained from a lawyer by using the site's e-mail link. A sample disclaimer is provided below.

Sample disclaimer for an Internet site:

---

1 http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

2 As an example: a person enquiring about the tax rate for France in a given year will receive information. If, on the other hand, a person enquires about his/her tax duties for a particular year, he/she will receive advice.

"The content of this site is for general information purposes only. It does not constitute professional advice (legal or otherwise) nor should it be used as such. We cannot accept responsibility for actions based on the material contained herein".

3. Links and references to third parties

If a site provides links and references the user of the site is likely to think the firm approves of the services and information provided on affiliate sites. Care must be taken to ensure that these sites do not appear offensive to the profession, or incompatible with the profession's underlying principles (e.g. if a law firm's website posts an advertisement or a link to an insurance company, it may give the impression that its independence is being jeopardised).

II. Lawyer correspondence

Professional lawyer correspondence is generally confidential. To protect the correspondence from being accessed by unauthorised parties, the CCBE suggests the following:

1. Deliberate interception and hacking

Lawyers have to protect the content of their electronic correspondence against any fraudulent modification, in particular to preserve their own interests.

To this end, it is recommended to lawyers to use means of electronic communication which are reasonably available to ensure the integrity and imputability of their electronic communications.

Although electronic communications are technically and legally protected against interception by third parties, their confidentiality might be in danger through various means. Lawyers have therefore to assess the risks encountered by their electronic correspondence and take appropriate measures, such as the use of encryption techniques according to the situation, and to inform their clients and correspondents of the risks encountered through electronic communications. Lawyers should not abstain from using encryption means reasonably available every time their client or correspondents request them.

2. Inadvertent access

Many firms already include a confidentiality warning on fax messages because of the risk that these will be sent to the wrong person by mistake. Firms should consider adopting similar confidentiality warnings for e-mail.

Automated confidentiality warnings

While automated confidentiality warnings are unlikely to impose any legally binding duty on an unintended recipient, many recipients may be expected to heed them, and the warnings may therefore help prevent a mistake from causing loss.

The following specimen warning is offered for adaptation:

"Information in this message is confidential. It is intended solely for the person to whom it is addressed. If you are not the intended recipient, please notify the sender, and please delete the message from your system immediately and thoroughly."

Firms can usefully attach this sample warning message to e-mail correspondence by using a template or a signature block.

Firms may feel that attaching such a warning to all e-mail correspondence is unnecessarily burdensome and may depreciate the importance of the warning. Nevertheless, unless lawyers consider whether to include the warning every time they send a message, it is recommended that the warning be attached to all e-mail correspondence.

Lawyers should note that legally confidential information in lawyer correspondence may cease to be confidential if the message is sent to others (for example, if the message is accidentally sent to a mailing list).

3. Viruses and malicious software

Electronic mail correspondence can be infected by viruses which can affect a firm's Internet site and entire network. In addition, such viruses and software can distribute confidential information or allow unauthorised access to it.

Firms are encouraged to have a security strategy and to maintain up-to-date technical precautions against such risks. They are also encouraged to ensure that users remain alert to the importance of security procedures. Some basic security procedures are included below:

(a) Adoption of anti-virus software.

(b) Configuring all outgoing e-mails so that attachments cannot open automatically upon receipt. This will ensure that viruses cannot be automatically imported into other systems.

(c) Ensuring the firm's computer network is adequately protected from incursions or viruses from the Internet.

If a firm is linked to the Internet through a permanent open line, it is strongly recommended that they install firewalls to ensure their systems are protected.

If a firm has a dial-in connection, it is recommended that it considers installing a firewall. If the expense is too high, the firm should at least consider isolating the computers which access the Internet from the firm's network. This will ensure that an incursion or virus from the Internet will not affect the firm's entire network.

(d) If the maintenance of a firm's network and computers is outsourced, it is recommended that the firm

- conducts appropriate security checks of the personnel who will be completing the maintenance work and ensures that the personnel have adequate technical qualifications;
- conducts adequate supervision of the work being carried out;
- agrees on measures to be taken for compliance with confidentiality and other ethical rules.

4. Electronic mail correspondence between lawyers

When sending an electronic mail correspondence, lawyers have to bear in mind the professional rules applicable to lawyers' correspondence in general. These professional rules may include rules on the form of the correspondence, or on the storage or archiving of the correspondence for a certain period of time, or again the confidentiality. Lawyers who send an electronic mail correspondence to a lawyer in another Member State and who wish that it remains confidential or without prejudice should clearly express his/her intention when communicating the document.

III. Safeguarding personal data: Data Protection Legislation

Lawyers should be aware that sending, receiving and holding e-mail correspondence may involve the processing of personal data which must be dealt with in accordance with Data Protection Legislation. This may include the obligation to notify the subject of the personal data about why their personal data

is being processed, who the data may be passed to and, in certain circumstances, the prior consent of the client may be required. The client may also be entitled to a copy of the data being processed.

At the very least, firms should include the following on the site and e-mails:

"Any personal data transmitted through our site may be stored on our databases for communication with you."

IV. Safeguarding copyright

Before downloading a file sent by e-mail, a lawyer should ensure that there will be no breach of copyright.

Example of a copyright notice:

"The content of this site is protected by copyright [© name of firm]. It cannot be copied, in part or in full, and in any form, unless it is done for the following purposes:

1) Personal use
Content of this site may be copied, in part or full, if the information is intended for personal use only.

2) Other purposes
The content of this site may be copied, in part or in full, for the benefit of a third party if all of the following conditions are met:

a) the copy indicates this site as its source and provides the site's complete address and copyright information;
b) the copy indicates that it is protected by copyright restrictions which must be respected by the third party;
c) the copy, in part or in full, must not be inserted into another text or publication, in whatever form, without prior permission;
d) the copy, in part or in full, must not be stored, on another website or on any other electronic system, without prior permission;
e) the copy, in part or in full, must never be disseminated for commercial purposes without prior permission.

No part of this site may be copied, transmitted or stored on another Web site or on any form of electronic system without prior permission, except for indexing and updating all search engines and similar services aimed at directing users to this website."

V. Best Practice Principles

There is no reason why firms should not give and receive professional undertakings by e-mail, but firms may wish to exercise caution when accepting any undertakings through this medium.

It is difficult to decide from the face of an e-mail message whether it was really sent by its purported sender, although its context may often put the matter beyond doubt.

In time, electronic signatures (eventually in connection with biometrics) will provide much better evidence of the authenticity of e-mail, and the widespread adoption of encryption will bring with it the additional benefit of improved authentication.

In the meantime, firms given a professional undertaking by e-mail are recommended to check that the context provides reasonable assurance of its authenticity, and/or to check by telephone or fax that it came from its purported sender.

E-mail: Automated confirmation of receipt: Firms are cautioned not to use automatic confirmation of the receipt of e-mails. It is important for the lawyer to send a confirmation only if the request for advice/information has been fully understood. He/she may well wish to ask the client for further information and agree on a timeframe in which the advice will be provided.

1. Knowing the Client

Firms may accept instructions by e-mail and via a website, but they should apply the same checks and make the same enquiries as they would for traditional client-lawyer communication (paper and face to face meetings).

The potential of the Internet for anonymous communications may prove attractive to fraudsters and money launderers, and firms must be alert to their duties in this area.

Some areas of practice, such as the making of wills and/or divorce on-line, present special risk when conducted remotely (impersonation or undue influence, for example), and e-mail may increase those risks and the need for caution.

2. Timely Response

a) Principles:

Firms already know (or should know) how to handle incoming letters, faxes and telephone calls in the absence of the intended recipient.

E-mail presents new problems because it can arrive unperceived by other members of staff. Firms are recommended to make effective technical and practical arrangements to ensure that e-mails receive a timely and appropriate response.

b) Guidance:

It is recommended that firms use automated out-of-office responses when staff is away from the office for a day or more provided that, in the same way, firms arrange for incoming e-mail, mails and faxes to be checked when the lawyer is absent. A limited number of people (a secretary and a colleague, for instance) should have access to an absent lawyer's inbox with a view to checking the contents regularly and ensuring that any urgent enquiries are dealt with promptly.

Systematically sending out-of-office messages in response to every e-mail received may be both annoying and a discredit to the firm, especially if an absent lawyer has subscribed to mailing lists and remains subscribed while on holiday. To avoid this, it is recommended that firms should, if possible, arrange for all automated out-of-office messages to be sent only once to every e-mail correspondent.

3. Spam

Unsolicited bulk e-mail or, as it is generally known, 'spam' can be a significant problem for firms using e-mail. Filtering software is available to reduce the amount of spam. However, if firms use spam filters they should warn clients in order to avoid that legitimate client correspondence has been blocked. They should explain that important communications should always be followed up with a phone call, fax or printed copy by post. Firms that run their own mail-servers (or whose Internet service provider will offer this service) should consider returning unsolicited e-mail to the sender with a message along the following lines: "Your message below was blocked by our filter because it was categorised as unsolicited bulk e-mail. If this was a mistake, we apologise. In that case, please send the message again, including in the header the access code *****. This will ensure that your message is not blocked and that the address from which you sent it is automatically recorded as one that should not be blocked in the future."

4. Records

Just as paper files are used to hold copies of outgoing letters and notes of telephone conversations, so copies of e-mail messages (other than those with no legal significance) should be kept on file. In respect to authenticity, the metadata of e-mail messages should be recorded as well. At this time, it is recommended that paper files be used although this view may change when the truly electronic office arrives.

Lawyers should be aware that even if an e-mail is deleted, it may still be capable of being retrieved. In disputes, even deleted e-mails may well be subject to disclosure.

For more detailed guidelines, please see paragraph VI.

5. User privacy

a) Principles:

Firms need to monitor the correspondence and communications of their fee-earners and other staff to ensure that their professional standards are maintained. If advice is given by staff by e-mail, firms will need to be able to check the accuracy of the advice.

Normally, this will be done by a review of paper files but cases may arise where firms will wish to check communications on their way to or from a member of staff.

Where the use of the firm's system for private communications is permitted, such a check may intrude on the privacy of members of a firm's staff. In certain jurisdictions, such checks may not be lawful.

b) Guidance for lawyers using e-mail:

If users are permitted to send private e-mail on the firm's system, it will be impractical to isolate it from other messages for monitoring purposes.

It should be part of the firm's terms of service that staff agrees to such monitoring, and the possibility of this occurring should be made clear.

6. Cross Border on-line: professional rules

If a lawyer provides his/her services via e-mail, the rules which apply to the lawyer - client relationship depends on the location of the lawyer[3]:
As an example:

- An Irish lawyer is giving advice, via e-mail, to a client in Belgium.
- The lawyer-client relationship is, in accordance with the E- Commerce Directive, governed by professional rules in Ireland.

If a lawyer provides his/her services, via e-mail, to a client who resides outside the EU, it is recommended that both parties agree on the rules to be applied to their relationship.

VI. Archiving of electronic documents and E-mails

Developments in information technology go fast and it is more and more common not to keep a paper copy of every document, but it is legally still necessary to archive certain documents and e-mail for several years. As is mentioned previously, lawyers should be aware that in disputes, even deleted e-mails may well be subject to disclosure.

---

[3] Directive 2000/31/EC of 8 June 2000 of the European Parliament and of the Council on certain legal aspects of Information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"): http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

1. Archiving e-mails

E-mail is an outstanding example of a distributed means of communication that is therefore difficult to control. Many people believe that e-mail has no official status. Employees often decide for themselves what should and should not be kept and save or delete their e-mail messages at their own discretion as they wrongly view electronic mail as part of their own personal working domain. Firms need to have fixed policies as to the choice of which e-mail messages need to be considered for preservation. In principle, the same criteria as for 'normal' paper post will apply. It will often depend as for paper of legal requirements in existence or statutory retention periods. There should also be guidelines for using and organising e-mail, as people simply printed them out and therefore they are not preserved correctly. Part of the context or other information is thus lost and the accessibility lessens.

2. Electronic signature[4]

As the use of digital signatures in documents and e-mails increases, the question of preserving the signatures also comes to the fore. Some of the data on which digital signatures are based and which to a large degree determine the trust that can be placed in a digital signature, is held by the accredited certification-service-providers in the sense of the EU Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures. This data is mainly data that proves the certification is genuine (data on consulted identity documents, application forms and signed conditions) and historical data about cancelled certificates. This data may be highly significant in the event of a dispute about the authenticity and applicability of a digital signature.

3. Authenticity

It is also important that the characteristics of the digital document be preserved so that the integrity of the document is safeguarded. This can be accomplished largely by developing a strategy in which the important aspects of the content, structure, appearance and the behaviour of the document can be preserved. The preservation of the characteristics of digital documents archived is very important. Finally, authentication is the important point. The context in which the document is made and used, and any changes that have been made as a result of management and preservation activities, are described in the metadata[5]. This makes it possible to demonstrate or verify the extent to which the document which has been archived is authentic in creation and contemporary use.

If the digital document is reproduced in a different computer environment than that in which it was originally made, it may look and behave entirely differently. If the transition to the other computer environment is not controlled, the authenticity of the digital document may be affected. Authenticity is a key concept in the preservation of documents, digital or other ways, and says that the document is what it says it is and that it was made by a specific person. The authenticity of documents can be safeguarded by describing and preserving the original context of the documents and by maintaining a chain of unbroken custody. A document has integrity when it is complete and uninterrupted in all essential aspects, so this means that it is intact and not changed or corrupted in such a way that its meaning is no longer clear. Changes are acceptable to a certain extent, as long as they do not affect the original meaning or function of the document. Basically, it makes no difference whether a document has a digital or a physical form: authentic preservation must be achieved, regardless. The problem that arises with digital documents, however, is that due to changing technology, not all aspects of a document can be preserved as precisely as when it was made. This does not mean, though, that sustainable preservation of authentic digital documents is impossible.

[4] See also directive 1999/92/EC on a Community framework for electronic signatures, OJ L13 of 19 January 2000, page 12.

[5] Not only the text of the document itself contains important data, also metadata is important. Metadata is data about data. Metadata is added to a digital document to describe extra information about the five characteristics of a document mentioned above so that, among other things, checks can be made on whether the document is what it 'says' it is. At the same time, metadata makes it possible to retrieve and use a particular digital document. Examples of such data are author of the document, subject, business process in which it was created and date on which it was created. But metadata is also important in the context of registering that preservation activities have been carried out.

As mentioned previously, archiving electronic documents and e-mails nowadays differs from how it used to be done for paper documents. When you keep the next points in mind when you create an e-mail or document, it will be easier to archive documents and e-mails, which need to be saved for several years according to legal requirements.

a) Document

When you keep in mind the next points it will be easier to archive[6] documents afterwards:

- use templates[7] to create documents
- start creating documents with a blank template, otherwise information (metadata[8]) of other documents might be included in the new document and will therefore include wrong information
- check if information in properties[9] screen is up-to-date
- instruct users to use explicit structure in documents, which means use of profiles/headings
- copy and paste as little as possible in order to prevent incorrect metadata to be included
- do not use passwords to secure documents, because if the password gets lost it is impossible to open the document, use read-only option instead
- use standard letter type fonts like Arial, or Times New Roman, because these fonts will be recognised by other programs
- use header and footer to insert metadata like name and version number of document
- do not use automatic date and time fields, because they may change every time you open the document
- use tables or tabs when necessary and not space bar, so the lay-out of the document is fixed
- save the document centrally on the server and not on the hard disk of the workstation, so the newest version can be retrieved by everyone

b) E-mail

In order to be able to decide if an e-mail needs to be archived, a distinction can be made alongside the following lines.

aa) Addressing e-mail messages

- always use the address book, because this contains extra information about the people to whom you are sending your message
- be circumspect when using distribution lists, because they can change often and if when the distribution list changes no information is kept about this, you cannot trace to whom the e-mail was sent to originally
- even if this sounds self-evident: always give your e-mail message a subject, it helps to sort and evaluate messages
- use message options like urgency only when absolutely necessary, because not all e-mail applications can reproduce them correctly

bb) Drafting an e-mail message

- where possible make and send messages in plain text or in HTML-format, because not all e-mail programs have the same possibilities in reading various fonts
- do not use automatically updating fields messages (not stable and may update every time the e-mail is opened)
- use attachments sensibly (send images as bitmap or .JPEG and not pasted in other application)
- do not 'insert' when replying to e-mail, just type your comments above the original message and leave space between headers of original message and your signature

[6] See paragraph about archiving.
[7] A template is a lay-out model for documents.
[8] See under 4.
[9] This option you will normally find under the heading 'file' of your word processing program. This option contains for example information about when the document has been created, by whom the document has been created and when the document has been adapted.

- use a signature block containing important contextual information so it is easier to trace the sender

cc) Managing e-mail messages

- ensure that the inbox is well managed, so when you receive a message decide if it needs to be saved and if so put it in the right folder
- if no special system exists to store messages, create directories for e-mails that have to be preserved to make tracing easier; make sure incoming and outgoing messages are kept in the same directory
- never paste content of message into another application and delete the original message as this would seriously damage both the authenticity and the integrity of the document (metadata[10] will get lost)

dd) Incoming or outgoing e-mail (internal and external)

This distinction has a different character to the classifications below, but is nonetheless relevant to the regulations for dealing with e-mail. A difference between internal and external e-mail can also be made in this category, distinguishing between electronic messages exchanged within an organisation and messages exchanged with outside parties.

ee) Official e-mail versus private e-mail

E-mail that an employee sends or receives as part of his/her job is official e-mail. E-mail that an employee sends or receives as a private individual, which is not related to the fact that the employee holds office in the organisation, is classified as private e-mail.

ff) E-mail to be preserved versus e-mail to be destroyed

If an e-mail message is functional, a decision has to be taken on whether it is eligible for preservation. In principle, the same criteria as for 'normal' paper post apply here too.

c) Archiving of documents and e-mail

It is advised to save the documents and e-mails in the original version with the program in which it is made, because it is not known what programs can do in the future with 'old' (digitally archived) versions of documents and e-mails. It is also recommended to use a generally accepted format, and to use this same format for all documents and e-mails. When archiving documents and e-mails, it should be kept in mind that both the preservation of their legibility for the future and the safeguarding of the documents and e-mails in their original versions are important.

[10] See under 4.