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

ELECTRONIC COMMUNICATION AND THE INTERNET

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

- Consider to use and offer appropriate means to protect the content of correspondence against any fraudulent modification, such as digital signatures or encryption, or both digital signatures and encryption
- Consider to use and offer a means of electronic communication, in particular when using web-mail service providers, online messengers or mobile devices, which is reasonably protected against any interception and hacking which could result in the disclosure of the existence and content of communications
- 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-mail

III. Safeguarding professional secrecy and personal data

- Sending, receiving and holding e-mail correspondence may involve the processing of personal data requiring sufficient data protection measures in order to comply with professional secrecy obligations and other applicable laws and legislation, which must be dealt with in accordance with relevant data protection legislation
- Display a confidentiality 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 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 for the appropriate time
- Be aware that saving electronic documents and e-mails in one program might have consequences for the possibility to retrieve them for the appropriate time
- Archive electronic documents and e-mails using a generally accepted format, ensuring their legibility in the future, and the safeguarding of the original version

VII. Awareness of hidden data in files and documents

- Be aware that files and documents may include hidden data that are not visible or which renders information about the document and is in addition to the main body of the text (often called "metadata")
- There might be meta data that it is useful or even vital for the lawyer to keep and other data that it is important to erase depending on where it is to be sent (eg the lawyer's file, to the client for tracking changes, or to the lawyer for the other party).
- Hidden data may be tied to visible data in such way, that copying and pasting visible data will also bring along the hidden data
- Always check whether "Track Changes" is used in electronic documents
- If using "Track Changes", make sure they are visible and "accept" or "reject" the changes before distributing the document unless the other party has intended to receive the document with such track changes visible.
- Check that no other version of the document is stored in the file
- Check "Document Properties" or similar before sending a document to see that it does not include information not intended for the recipient
- Use specific programs that permits the analysis of and to strip out hidden data
- Consider installing a system that automatically checks outgoing electronic documents and removes hidden data

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 for advertising, but also as a means of disseminating legal advice and information. Many lawyers feel that providing legal services on-line offers the opportunity to obtain access to 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), and a person could wrongly portray him/herself as a lawyer, as has occurred in the physical world.

4. The archiving of electronic documents and e-mails is an issue of great importance. The CCBE therefore consider 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 suitable 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 in public discussions on mailing lists by e-mail, confidentiality or privilege warnings are obviously inappropriate, and their inclusion can detract from the effect 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.

---

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.

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:

"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 that lawyers use a means of electronic communication that is reasonably available to ensure the integrity 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 (in particular when using web-mail service providers, online messengers or mobile devices) 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 that is 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 e-mail servers 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 obtain access to 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 the confidentiality. Lawyers who send correspondence by electronic mail 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 lawyer client privilege and personal data

Lawyers should be aware that sending, receiving and holding e-mail correspondence may involve the processing of personal data, requiring sufficient data protection measures to be in place in order to comply with professional secrecy obligations and other applicable laws and legislation. .

IV. Safeguarding copyright

Before downloading a file, a lawyer should ensure that there will be no infringement 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."

Other exemptions may also apply in accordance with local circumstances.

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, digital signatures (eventually in connection with biometrics) may 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 should there be any doubts about this.

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 or 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. Firms should be aware that it may be necessary to positively disable this function in the e-mail program options.

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 members of staff are 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 the blocking of legitimate correspondence. They should explain that important communications should always be followed up with a telephone call, fax or printed copy by post. Firms that run their own mail-servers should consider returning unsolicited e-mail to the sender with a message along the specified lines

4. Records

Just as paper files are used to retain 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 members of 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 members of staff agree 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 gives 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 increasingly common not to keep a paper copy of every document, but it remains legally 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. The requirements set out in law that apply to documents in paper format will also apply to documents in electronic format. The format of the document is irrelevant. There should also be guidelines for using and organising e-mail, as people tend to print 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 the purported 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 differs from how paper documents are archived. 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 the information in the properties[9] screen is up-to-date
- instruct users to use explicit structure in documents, which means use of profiles and headings
- copy and paste as little as possible in order to prevent incorrect metadata being 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 headers and footers to insert metadata such as 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, taking into account the following comments.

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, such as '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 can read 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)

[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.

- 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
- 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 as to 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.

VII. Awareness of hidden data in files and documents

It is important to be aware that electronic documents and other computer files often carry additional information which renders information about the document or about its purported author, and that may be open or hidden, e.g. author, date and time of creation and last change, template used and such like. Depending on the nature of information and the context in which it later appears, the information may be useful, harmless or embarrassing, potentially dangerous or lead to an accidental disclosure of confidential information or information not intended for the recipient of the document. On the other hand, such data could also be useful or even vital to keep for a lawyer. In this case, the lawyer would need to take steps to preserve the metadata and to not to let it out to other parties.

a) Document re-use and information disclosure

Lawyers are experts in reusing documents, and it is very common to use a document as a starting point when creating another document in another case for another client, and the new document as a

[10] See under 4.

new starting point in yet another case for yet another client. If the lawyer is not aware of the existence of hidden data, it is possible that the recipient of the last version of the document, by analysing the hidden data, can tell who the original document was created for and which changes or amendments have been made by the various individuals having reviewed it. Copying the contents of a document and pasting them into a new document is not a reliable method to avoid that hidden data are following the document, as some hidden data are tied to a text in such way that pasting the text into a new document will also copy the original hidden data.

b) Multiple versions of content

The "Track Changes" function in Microsoft Word is useful to see changes made between document versions, but this feature must be used with due caution. "Track Changes" might be turned on, but the user might have change display switched off and as a result the changes made and by whom may be visible when change display is switched on again.

As a general guideline it is suggested that users always check whether "Track Changes" is used or not. The only way to discard saved changes between document versions is either to accept them or to reject them.

c) Regarding using PDF instead of Microsoft Word for Distributing Documents

PDF documents are a good alternative to documents in Microsoft Word format. For the most part, PDF is immune to the mentioned issues, as PDF documents really represent the document as it will be printed. Note however, that e.g. inserting a black or white box over a text will not remove the text, but place that box over the text and thus hide the text when printed. By removing the box, the text will be visible again. PDF documents do support a number of user-specified hidden data, but in practice use of such data is very unusual. To be on the safe side, however, it's recommended that "Document Properties" are checked before distributing the document.

It should be noted that there are different kinds of PDF document. A PDF document created by scanning text using a scanner or photocopier may contain only an image copy of the markings on the sheet of paper. The text in such a document cannot be searched using word-searching tools and cannot easily be cut and pasted into other documents. On the other hand, a PDF document saved from a word-processing program is usually stored as text and not simply as an image. Documents in this form require less storage space than image PDF documents. For these reasons, documents should generally be saved as text PDF documents (as opposed to image PDF documents) where they are to be stored in a searchable database, or where limiting file sizes (for example in e-mail attachments) is important.

d) Special tools to remove hidden data

There exist special computer software tools that analyse documents and can remove old versions of content or other hidden data. It is recommended that these tools are installed and used when distributing sensitive information in electronic documents. These tools can be downloaded for example from the web-site of Microsoft and be installed in the Office2003/XP version. In the Office 2007 version of Word, this is already a default tool (please see "Office button"/"Inspect Document").