COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 27 July 2016 CDCJ(2015)14 final

EUROPEAN COMMITTEE ON LEGAL CO-OPERATION
(CDCJ)

THE USE OF ELECTRONIC EVIDENCE IN CIVIL AND ADMINISTATIVE LAW PROCEEDINGS AND ITS EFFECT ON THE RULES OF EVIDENCE AND MODES OF PROOF

A comparative study and analysis

Report prepared by Stephen MASON

Assisted by Uwe RASMUSSEN

CONTENTS

Page

The authors

Stephen Mason

Stephen Mason is a barrister, an Associate Research Fellow at the Institute of Advanced Legal Studies in London, and a member of the Information Technology Panel of the General Council of the Bar of England & Wales.

He is the general editor of *Electronic Evidence* (3rd ed, LexisNexis Butterworths, 2012) and *International Electronic Evidence* (British Institute of International and Comparative Law, 2008).

He is also the author of *Electronic Signatures in Law* (3rd ed, Cambridge University Press, 2012); *Electronic Disclosure A Casebook for Civil and Criminal Practitioners* (PP Publishing, 2015); *Email, social media and the Internet at work: A concise guide to compliance with the law* (7th ed, PP Publishing, 2014), and *When Bank Systems Fail Debit cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* (2nd ed, PP Publishing, 2014); and

He founded the international open source journal *Digital Evidence and Electronic Signature Law Review*, which has become an international focal point for judges, lawyers and researchers.

Stephen has acted as the external marker in postgraduate degrees dealing with electronic evidence: LLM at the University of Oslo (2006); PhD at the University of Exeter (2013), and a PhD entitled 'Authentication of Electronic Evidence' at Queensland University of Technology, Brisbane, Australia (October/November 2015).

Uwe Rasmussen

Uwe Rasmussen is French attorney specialized in Information Technology law, electronic evidence, personal data protection, compliance, and database rights.

He is a co-author of the Council of Europe's guide on Electronic Evidence.

He is regional counsel to a large software multi-national on Internet law and evidence cooperation processes. Mr Rasmussen holds law degrees from the Sorbonne in Paris and Copenhagen University and has studied Intellectual Property law at Santa Clara University and is moreover a Microsoft Certified Systems Engineer.

Introduction

1. The Council of Europe commissioned a report, covering a comparative study and analysis of existing national legal provisions that have been adopted or adapted on the effect of electronic evidence on the rules of evidence and modes of proof, with a focus on proceedings relating to civil law, administrative law and commercial law (for the purposes of making the analysis slightly easier, 'civil law' and 'commercial law' are considered to be 'civil proceedings').

2. The aim of the study is to identify the problems that the different legal systems in the member states are faced with in this field and in respect of which they are in need of remedies or in respect of which they have put in place solutions.

3. The initial Terms of Reference (see Appendix A to this report) required that study should deal, but not exclusively, with issues relating to the following:

- The admissibility of electronic evidence
- The weight given to electronic evidence
- The implications for credential rules such as:
  - Burden of proof
  - Presumptions
  - Authenticity/reliability
  - Archiving and preservation of evidence
  - Case and trial management
  - The role of the judge
  - Pre-trial search for evidence
  - The role of independent or court experts.

4. Ideally, the study was to cover all 47-member states of the Council of Europe. For this reason, a series of questions were devised to send out to the members of the European Committee on Legal Co-operation, so that they can respond within a time frame that enabled the authors to prepare the draft report to be submitted before the end of 2014.

Purpose of the study: a change of outlook

5. The purpose of the study is to encourage judges, lawyers and jurists to understand that it is necessary to change their outlook regarding this new form of evidence.[1]

6. Recording content on paper means the medium and the content are bound together. Digital information is completely different.[2] At its basic level, 'bits and bytes' comprise the content, that is, 0s and 1s. In addition, the medium can be many disparate devices, and software written by human beings is required to read and interpret the data. This means it is necessary for us to grasp the need for a conceptual change. With its unique characteristics, complex questions about the integrity and security of electronic evidence may be raised, although the authentication of complex forms of electronic evidence will differ to less complex forms of electronic evidence, such as e-mails or text messages, for instance.

7. The taxonomy for traditional forms of evidence is well established. However, the taxonomy regarding electronic evidence is still evolving, and at present it includes the following elements:[3]

Understanding the digital realm
- Sources of digital evidence
- Characteristics of digital evidence
- Encrypted data

Authenticity
- Proof (including the investigation, seizure and examination of digital evidence)
- 'Reliability' and presumptions
- Authenticity
- Integrity

Software as the witness (known as hearsay in common law systems).

8. As will be readily observed, there are some areas of knowledge included in the list above that are not included in a conventional textbook on evidence. The additional items reflect the nature of electronic evidence. For instance, a more considered approach is necessary regarding how electronic evidence is seized, investigated and examined. This is because this initial process can be so flawed as to render the evidence inadmissible or open to challenges, especially regarding its authenticity.

[1] For discussion of the importance of the topic in legal education, see Denise Wong, 'Educating for the future: teaching evidence in the technological age', *Digital Evidence and Electronic Signature Law Review*, 10 (2013) pp. 16 – 24 and Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', *Digital Evidence and Electronic Signature Law Review*, 10 (2013) pp. 23 – 28.

[2] At present, there is no generally agreed term relating to the form of evidence that comes from our use of technology: specifically, software. For the sake of shorthand, the words 'electronic' and 'digital' are used interchangeably. For a detailed discussion of these terms, see Burkhard Schafer and Stephen Mason, Chapter 2, 'The characteristics of electronic evidence in digital format' in Stephen Mason, gen ed, *Electronic Evidence* (3rd ed, LexisNexis Butterworths, 2012).

[3] This is taken from Stephen Mason: 'A framework for a syllabus to teach electronic evidence', *Digital Evidence and Electronic Signature Law Review* 10 (2013), pp. 7 – 15; see also Stephen Mason, 'The structure of electronic evidence: have we got it right?', *Editorial, Amicus Curiae* The Journal of the Society for Advanced Legal Studies, Issue 99, Autumn 2014, 1.

Proposal

9. The Terms of Reference requested:

(i) An analysis of existing national legal provisions that have been adopted or adapted on the effect of electronic evidence on the rules of evidence and modes of proof, with a focus on proceedings relating to civil law, administrative law and commercial law.

(ii) To identify the problems that the different legal systems in the member states are faced with in this field and in respect of which they are in need of remedies or in respect of which they have put in place solutions.

(iii) To draw up proposals for solutions on the basis of approaches and best practice already adopted in member and other states with the objective of solving or at least reducing the workload of courts in dealing with electronic evidence in civil and administrative law proceedings.

10. The issues set out below were initially included in the first questionnaire. They are set out in order of how they would be considered as legal proceedings begin. The role of the judge begins when there is an application for a search of evidence, should a search be necessary. In this respect, it is taken as a given that the role of the judge needs to be considered throughout the process and in connection with each of the issues identified below:

Pre-trial search for evidence

Preservation of evidence

Case and trial management

The role of the independent or court expert witness

Burden of proof (this will be relevant when drafting pleadings, as it is relevant when conducting the case in court)

Substantial issues regarding the nature of the evidence:
- Admissibility
- Presumptions
- Authenticity and reliability
- Weight

The archiving of evidence after trial.

11. The aim of the study is to identify the *problems* that the different legal systems in the member states are faced with in this field, together with the *remedies* or *solutions* that have been put in place.

12. As a preliminary step, it was necessary to establish what action, if any, member states had already undertaken to deal with the areas set out above. Drawing upon the analysis, a number of recommendations were considered to take the matter further.

Initial questionnaire

13. The authors prepared a series of questions relating to each of the issues to be considered in the study. In order to help member states in replying to these questions, the authors prepared a model analysis of the position in England & Wales and in France. This model analysis was attached to the proposed questionnaire in the form of two separate annexes. The aim of asking such questions was to obtain a reasonably accurate understanding of how each member state had responded to the problems that have arisen.

Revised questionnaire

14. At the 89th meeting of the European Committee on Legal Co-operation (CDCJ) held in Strasbourg on 29-31 October 2014, the members of the committee requested the authors to prepare a simplified questionnaire (focusing on challenges and procedural changes only) [see B-11].

15. The authors subsequently prepared a revised questionnaire (reproduced in Appendix B to this report), and the Secretariat posted the questionnaire on the Council of Europe website and sent this questionnaire to the following organisations on 13 March 2015:

Bar associations in Council of Europe member States
Notary Chambers in Council of Europe member States
Council of the Notariats of the European Union
Association européenne des magistrats
Conseil des Barreaux européens (CCBE)
Magistrats Européens pour la Démocratie et les Libertés (MEDEL), a group of European magistrates, judges and prosecutors.

European Informatics Data Exchange Framework for Courts and Evidence

16. Stephen Mason alerted the members of the CDCJ to the European Union (EU) project *European Informatics Data Exchange Framework for Courts and Evidence* (e-Evidence).[4] The Committee requested the work of this project to be noted in the study.

17. The project began its activities in Florence in March 2014 and will produce its final results in October 2016. The project will consider a common legal response, and to recommend standard procedures in the use, collection and exchange of electronic evidence across EU member States. Guidelines, recommendations and technical standards will be proposed, including a proposed digital evidence exchange in accordance with common standards and rules.

18. The following objectives are considered essential:

(i) Developing a common and shared understanding on what electronic evidence is and the relevant concepts of electronic evidence involved (digital forensics, criminal law, criminal procedure, criminal international cooperation) (Work Package 2: mind map categorization).

(ii) Establishing rules and criteria for the processing of electronic evidence in EU Member States, and how the exchange of evidence should be regulated (Work Package 3: legal issues).

[4] http://www.evidenceproject.eu.

(iii) Providing for criteria and standards to guarantee the reliability, integrity and chain of custody requirement of electronic evidence in the EU Member States and in the exchange of such evidence (Work Package 4: standard issues).

(iv) Setting out the implications by providing an overview and current assessment of the collection, preservation and exchange of electronic evidence from the point of view of law enforcement agencies, and proposing guidelines that could be integrated into a Common European Framework governing this field (Work Package 6: law enforcement issues).

(v) Considering the implications for data privacy (Work Package 8: data protection issues).

(vi) Identifying and developing technological functionalities for a Common European Framework in the gathering and exchange of electronic evidence (Work Package 5: technical issues).

(vii) Considering the issues relating to the seizure of electronic evidence (Work Package 7: market size).

19. Steps (i), (v) and (vii) are almost complete. Steps (ii), (iii), (iv) and (vi) continue to be developed.

Responses received

20. Responses were received from the Ministry of Justice of: Andorra; Armenia; Belgium; Croatia (who updated the response submitted in respect of the initial questionnaire); Czech Republic; Denmark; Finland; France; Germany; Hungary; Ireland; Italy (who submitted a response to the initial questionnaire); Latvia; Lithuania; Malta; Montenegro; Norway; Poland, Portugal; Romania; Russian Federation; Serbia; Slovak Republic; Spain; Sweden; Switzerland; Turkey, Ukraine and the United Kingdom (dealing with England & Wales).

21. Further responses were received in respect of: Andorra from the *Col.legi d'Advocats d'Andorra;* Bulgaria from the Supreme Judicial Council of Bulgaria; Georgia from the High Council of Justice; Germany from the Federal Chamber of Notarie; and Spain from *Services Juridiques du Consejo General de la Abogacía Española*.

22. Individual lawyers sent responses for Armenia (Anahit Beglaryan, Advocate, member of the Chamber of Advocates), Estonia (Mr Maksim Greinoman, a partner of Advokaadibüroo Greinoman & Co, Tallinn) and Greece (Michael G. Rachavelias, Attorney at law, member of the Larissa Bar Association).

Practical notes

23. The questionnaire was directed to the use of electronic evidence in civil and administrative proceedings. Where a response included a reference to criminal proceedings, the element dealing with the position in criminal proceedings was ignored.

24. Croatia and Italy answered the questions in the first questionnaire, which means that some of the questions in the revised questionnaire are not answered by either member state.

25. It was not clear how some of the questions were answered by a number of member states, in that the answer (yes/no) did not appear to be consistent when considering the additional commentary provided, or some questions were answered 'yes' and 'no'. Some of the questions were interpreted in different ways by those responding to the questionnaire on behalf of their state, which might account for the discrepancy in the response. Also, some responses inferred that we had asked the wrong question: such a response is quite possibly correct, given the breadth of substantive law and procedural rules that we were canvassing via the questionnaire. In addition, some member states did not answer every question. As a result some of the answers have been interpreted.

26. Where there was a difference in answer between two separate responses from the same member state, the answer by the relevant Ministry of Justice has been preferred.

Analysis of the responses

27. In the analysis of responses, the preamble and questions of the revised questionnaire are set out in full.

Part A Obtaining electronic evidence

Preamble

28. There are three types of evidence that might need to be obtained in legal proceedings:

(i) Evidence from publicly available websites, such as (this list is only indicative) blog postings and images uploaded to social networking websites.

(ii) The substantive evidence (or evidence of content), that is the e-mail or documents in digital format that are not made publicly available and which are held on a server.

(iii) Purported user identity and traffic data ('meta data') that is used to help identify a person by finding out the source of the communication, but not the content.

29. For instance, a jurisdiction problem arises if a French company believes an employee has stolen trade secrets and stored the data on a British private cloud service.

30. Question 1
If a party wants to submit evidence from publicly available Internet websites, will a court customarily require that the copies of websites be collected in a specific manner to ensure the authenticity such as the use of a process server or a court appointed digital evidence specialist?

Analysis of responses to question 1

31. In five member states: Andorra, Croatia, France, Lithuania and Turkey, the rule in each jurisdiction is more nuanced than a strict answer of 'yes' to the question, as indicated below:

(i) In Andorra, the evidence has to be collected in a specific manner only in the event of a challenge by an opposing party. A notary will usually be asked to certify the website.

(ii) In Croatia, article 234 of the Civil Procedure Act provides that when a judge requests evidence, a third party is required to submit the document. The document then becomes a joint document for that person and the party that refers to the document.

(iii) In France, a party may submit a copy of a website or a screenshot, particularly to prove the existence of a legal fact. However, the court may consider it necessary to order additional measures so as to clarify questions of fact in accordance with article 10 of the Code of Civil Procedure. Within this framework, the court may appoint any person of its choice to advise it by means of findings, consultation or expertise. For instance, a bailiff may also be appointed by the court to produce a report, but the scope of this assignment is extremely limited as it is confined to making mere findings of fact, entered into an official report. The bailiff's report is

authoritative failing evidence to the contrary. An expert may also be appointed by the court to advise it on the reliability of a copy of a website or a screenshot or to make such copies.

(iv) In Lithuania, the rule is that original documents should be submitted, and if copies are submitted, then a court, a notary or a lawyer participating in the case must certify the copies.

(v) In Turkey, it is only if the court handling the case has doubts about the authenticity of the evidence or the parties have objections on this issue, that the court would customarily require that the copies of websites be collected in a specific manner to ensure authenticity.

32. The remaining member states responding to the questionnaire indicated that there were no requirements to collect electronic evidence in a specific manner.

33. The response from Armenia is interpreted to mean that there are no specific procedures, but in practice, the lawyers submitting the response for Armenia indicated that they mention the Internet link, so the court has the opportunity to check the evidence through the link and ensure the authenticity of the data. In addition, article 60 of the Code of Civil Procedure and article 37 of the Code of Administrative Procedure stipulate that, in order to clarify issues requiring specialized knowledge that arise during a trial, the court can, by motion of a party, or both parties, or by its own initiative, appoint an expert examination, which may be assigned either to a professional expert institution or to a professional expert.

(i) The response by Greece indicated that previously there were requirements in place, but it seems that the present position is that there are no longer any requirements, because previously there was an emphasis on the need for tangible evidence.

(ii) The Polish delegation indicated that Polish law does not provide for a definition of ‘electronic evidence’. Neither administrative nor civil or criminal procedure codes contain such definition or its equivalent. Every request for the production of evidence and evidence as such is considered from the point of view of its usefulness to prove or deny the statement (article 75 of the Administrative Procedure Code, or article 227 of the Civil Procedure Code). All evidence (every request for the production of evidence) is subject to evaluation by the authority in charge of proceedings. The parties may question the evidence. They are also entitled to present new motions on particular evidence. Polish procedural law disregards the legal evidence theory, although some constraints may be found in the case law.

34. Question 2
Is it possible for a party to apply to a court to obtain a copy of electronic data (such as computer files stored on a computer of a third party within the jurisdiction) before a legal action has been initiated on the merits?

Analysis of responses to question 2

35. In Armenia, Malta and Serbia, it is not possible for a party obtain a copy of electronic data before a legal action has been initiated on the merits. In Andorra, the Ministry indicated that it is not possible for a party obtain a copy of electronic data before a legal action has been initiated on the merits, but the Col.legi d'Advocats d'Andorra indicated that it was possible.

36. Of the remaining jurisdictions that answered the question, a party can apply to a court to obtain a copy of electronic data, although different rules might apply depending on whether the evidence is to be obtained where a party is likely to be a party to the action; where the party is not likely to be a party to the action, where a person who is mixed up in wrongdoing, or where the relevant Procedural Rules set out criteria that must be considered before any such application.

37. In England & Wales, the Civil Procedure Rules and case law cover this eventuality, but in some jurisdictions, such as Estonia, it is only available in exceptional circumstances through the preliminary evidence collection procedure, and very rarely granted in practice. In Latvia, a party can petition the court to secure evidence in both administrative and civil proceedings where they have cause to believe that it might be impossible or problematic to obtain the evidence in the future. The position is similar in Lithuania, where a party can apply to the court to apply protective measures to safeguard evidence in accordance with articles 144 and 221 of the Code of Civil Procedure.

38. Question 3
Is it possible for a party that is not resident in your country to apply for the same court order as mentioned in 2 above, and is it also possible even if it is unlikely that the legal action on the merits will be litigated before a national court?

Analysis of responses to question 3

39. With the exception of Malta and Serbia, it is possible for a party in other member states that is not resident in the jurisdiction to apply for the same court order as mentioned in question 2 above. In Andorra, the Ministry indicated that it is not possible, but the Col.legi d'Advocats d'Andorra indicated that it was possible.

40. Question 4
When seizing electronic evidence pursuant to a court order, is the party seeking the evidence obliged to follow any particular set of legal provisions or guidelines for seizing electronic evidence?

Analysis of responses to question 4

41. No guidelines apply to the seizure of electronic evidence in civil proceedings, although in Croatia it is necessary to make an application to the court to seize evidence; in the Czech Republic any steps concerning evidence must be undertaken in accordance with the Civil Procedure Code, and evidence is safeguarded by the court; in Estonia, a bailiff will enforce an order; in France the bailiff notifies the person in possession of the evidence and also collects the evidence, and in Portugal it may be necessary for the court to provide for such formalities.

42. Question 5
Regarding administrative proceedings, please indicate whether there are any special rules regarding the submission of evidence, especially regarding electronic signatures, and whether a specific form of electronic signature is required when submitting evidence electronically.

Analysis of responses to question 5

43. There are no special rules for many of the jurisdictions that responded to the questionnaire. In Croatia, a third party is required to submit evidence at the request of the court. In Estonia, documents should be signed using the Estonian digital signature, although in practice, submissions may be made without a signature. In Poland, submissions must be certified in accordance with the provision of the law on the digitalization of the public authority activities and comply with a specific format and contain the electronic address of the sender.

Table 1

Responses to questions 1 – 5

	1		2		3		4		5
	Yes	No	Yes	No	Yes	No	Yes	No	
Andorra	✓			✓		✓		✓	There was no response from the Ministry, but the Col.legi d'Advocats d'Andorra indicated there was no provision in the legislation.
Armenia		✓		✓	✓			✓	There are no special rules on the submission of electronic evidence, but amendments are expected to the Civil Procedure Code and Administrative Procedure Code.
Belgium		✓	✓		✓		✓		There are no special rules on the submission of electronic evidence.
Bulgaria	✓		✓		✓			✓	There are no special rules on the submission of electronic evidence.
Croatia	✓		✓		✓			✓	The Civil Procedure Act stipulates that an electronic document must be signed with an advanced electronic signature submitted on a prescribed form and sent electronically to the central information system.
Czech Republic		✓	✓		✓		✓		Administrative proceedings are in general subject to rules imposed by the Administrative Procedure Code (Act N°500/2004 Coll.). Section 37 paragraph 4 of the Code requires that a document submitted to an administrative authority by electronic means is provided with an electronic

									signature. Act N°300/2008 Coll. on Electronic acts and on Authorized Conversion of Documents provides exemptions when a natural person or legal entity is not obliged to provide their submission with an electronic signature. According to the provisions of section 18 paragraph 2, a document submitted by means of a certified data mailbox does not have to be provided with an electronic signature. Such an act has the same effects as an act made in writing and signed.
Denmark		✓	✓		✓			✓	There are no special rules.
Estonia		✓	✓		✓			✓	Documents should be signed using the Estonian digital signature. In practice, submissions may be made without a signature.
Finland		✓	✓		✓			✓	There are no special rules. See the response for more detail regarding precautionary measures, including the answer to question 2.
France	✓		✓		✓			✓	No response.
Georgia		✓	✓		✓			✓	No response.
Germany		✓	✓		✓			✓	Generally it is possible to submit electronic data in administrative proceedings without meeting a specific form. Only where the law requires written form must electronic documents be signed with a qualified electronic signature, see para 3a of the German Administrative Procedures Act. See the accompanying compilation of responses for more detail.
Greece		✓	✓		✓			✓	According to article 4 of Presidential Decree 150/2013, every electronic file that is submitted in courts, no matter of its format, must be submitted with the use of an advanced electronic signature. See the response for more detail.
Hungary		✓	✓		✓			✓	There are no specific procedures set for the submission of electronic evidence, although certain presumptions apply to private and public documents when certain forms of electronic signature are used. See the accompanying compilation of

									responses for more detail.
Ireland		✓	✓		✓			✓	There are no specific procedures set for submission of electronic evidence.
Italy					✓				No response.
Latvia		✓	✓		✓			✓	Where evidence is submitted electronically, it is necessary for the data to be signed with an advanced electronic signature.
Lithuania	✓		✓		✓			✓	There are no special rules. See the accompanying compilation of responses for more detail.
Malta		✓		✓		✓		✓	There are no special rules relative to administrative proceedings and the submission of electronic evidence.
Montenegro		✓	✓		✓			✓	There are no special rules. See the accompanying compilation of responses for more detail.
Norway			✓		✓				See the accompanying compilation of responses for more detail.
Poland		✓	✓		✓			✓	There are no special rules. See the accompanying compilation of responses for more detail.
Portugal		✓	✓		✓		✓		There are no special rules. See the accompanying compilation of responses for more detail.
Romania	✓		✓		✓			✓	The relevant provisions regarding the submission of electronic evidence, especially regarding electronic signatures, are contained in Law No. 455/2001 on electronic signature. In administrative proceedings, the provisions relating to the legal status of electronic written documents apply (Law No. 455/2001 on electronic signature, articles 5 to 11).
Russian Federation		✓	✓		✓			✓	There are no special rules. See the accompanying compilation of responses for more detail.
Serbia		✓		✓		✓		✓	Article 21 of The Law on Administrative Disputes provides provisions about submission and treatment of electronic documents that are closely defined by the Court Rules of Procedure.

Slovak Republic		✓	✓		✓			✓	There are no special rules. See the accompanying compilation of responses for more detail.
Spain		✓	✓		✓			✓	See the accompanying compilation of responses for more detail.
Sweden		✓	✓		✓			✓	There are no special rules.
Switzerland		✓	✓		✓			✓	There are no special rules.
Turkey	✓		✓		✓			✓	The Administrative Jurisdiction Procedures Law regulates administrative disputes. The Code does not include a specific legislation about submitting evidence.
Ukraine		✓		✓		✓		✓	There are no special rules.
UK (England & Wales)		✓	✓		✓			✓	There are no special rules.

Part B Obtaining purported user identification

Preamble

44. The problem arises when a party claims that an e-mail message caused damage (defamation, trade secrets, etc.) but the identity of the sender cannot be ascertained. The party that has suffered a wrong uses the identifying information from the e-mail provider (meta-data) to prove the connection between an e-mail account and a natural person, that is, the e-mail user.

45. Question 6
Is it possible for a party to apply to a court to identify the user of an electronic service provided by a company within your jurisdiction, such as the user of an e-mail account, Internet access service, or VoIP account?

Analysis of responses to question 6

46. All those responding with the exception of Croatia, Finland, Georgia, Malta, Serbia, Slovak Republic and Ukraine indicated that a party could apply to a court to identify the user of an electronic service provided by a company within their own jurisdiction. In Andorra, the Ministry indicated that it is not possible, but the Col.legi d'Advocats d'Andorra indicated that it was possible. In Belgium, there are number of alternative methods that can be used to elicit the information, and the reader is directed to the Belgian response to the questionnaire for more details. In the Czech Republic, the deciding factor is the jurisdiction, and whether the matter falls within the jurisdiction of the court, and in Hungary, the position is dependent upon how the Information Act is interpreted.

47. Question 7
Is it possible for a party that is not resident in your country to apply for the same court order, and is it also possible if it is unlikely that the legal action on the merits will be litigated before a national court?

Analysis of responses to question 7

48. All those responding with the exception of Belgium, Croatia, Finland, Georgia, Malta, Russian Federation, Serbia, Slovak Republic and Ukraine indicated that a party that is not resident in the jurisdiction can apply to a court to identify the user of an electronic service provided by a company within the jurisdiction, and it is possible to initiate legal action on the merits. In Andorra, the Ministry indicated that it is not possible, but the Col.legi d'Advocats d'Andorra indicated that it was possible.

49. In the Czech Republic, the deciding factor is the jurisdiction, and whether the matter falls within the jurisdiction of the court. In Hungary, the position is dependent upon how the Information Act is interpreted. In the case of Latvia, the petition can only be submitted once the court has accepted the applicant and action has been initiated. In Lithuania, a party can apply to the court to apply protective measures before legal action is initiated to safeguard evidence in accordance with articles 144 and 221 of the Code of Civil Procedure.

Table 2

Responses to questions 6 and 7

	6		7	
	Yes	No	Yes	No
Andorra		✓		✓
Armenia	✓		✓	
Belgium		✓		✓
Bulgaria	✓		✓	
Croatia		✓		✓
Czech Republic	✓		✓	
Denmark	✓		✓	
Estonia	✓		✓	
Finland		✓		✓
France	✓		✓	
Georgia		✓		✓
Germany	✓		✓	
Greece	✓		✓	
Hungary	✓		✓	
Ireland	✓		✓	
Latvia	✓		✓	
Lithuania	✓		✓	
Malta		✓		✓
Montenegro	✓		✓	
Norway	✓		✓	
Poland	✓		✓	
Portugal	✓			
Romania	✓		✓	
Russian Federation	✓		✓	
Serbia		✓		✓
Slovak Republic		✓	✓	
Spain	✓		✓	
Sweden	✓		✓	
Switzerland	✓		✓	
Turkey	✓		✓	
Ukraine		✓		✓
UK (England & Wales)	✓		✓	

Part C Substantive issues regarding the nature of electronic evidence

Preamble

50. To a certain extent, electronic evidence is a still relatively new concept. The aim in asking questions in this section is to assess how different jurisdictions are dealing with electronic evidence in legal proceedings. Article 9 of the EU Directive 2000/31 on E-Commerce requires Member States to allow for electronic contracting in a manner that it does not create obstacles for their validity; see also article 4-2 of the EU Directive 1999/93 on Electronic Signatures.

51. Question 8
Please set out the classifications of evidence, if any, and how electronic evidence fits into the classification. For example, are certain types of electronic evidence presumed authentic and reliable and are there other types that are presumed unreliable?

Analysis of responses to question 8

52. For the detailed explanation for each jurisdiction, please see the individual response and the outline provided in the table to this question, but generally evidence is presumed reliable unless challenged.

53. Question 9
Is there a presumption in your jurisdiction relating to electronic evidence regarding it being "reliable", "in order", "accurate", "properly set or calibrated" or "working properly"?

Analysis of responses to question 9

54. There is such a presumption in England & Wales, introduced by the Law Commission, but it is the topic of criticism.[5] The presumption that all evidence is presumed reliable applies in Estonia, with the proviso that if the opposing party challenges the evidence, then the evidence must be authenticated. In Hungary, the position will depend on the methods used to sign the document. The position is not certain in Montenegro. In Romania, article 265(a) of the New Code of Civil Procedure provides that 'the entry of data from a legal instrument on a computer is presumed to provide sufficient meaningful guarantees as to its reliability if it is carried out systematically and without gaps and where the computerised data are protected against alterations and counterfeiting so that the integrity of the document is fully ensured'. In the Russian Federation, there is a presumption where electronic data are obtained in the manner prescribed by law. In Portugal and Spain a presumption will apply, depending on whether data in digital format is 'signed' by an advanced electronic signature. There is no such presumption in the other jurisdictions submitting responses to the questionnaire.

[5] For a detailed critique, see Stephen Mason, gen ed, *Electronic Evidence* (3rd ed, LexisNexis Butterworths, 2012) chapter 5.

Table 3

Responses to questions 8 and 9

	8	**9**	
		Yes	No
Andorra	The parties must adduce electronic evidence as private documentary evidence, which makes it possible for the opposing party to challenge it by producing other evidence of a similar nature.		✓
Armenia	Electronic evidence is classified as written evidence, for which see article 54 of the Civil Procedure Code.		✓
Belgium	The Belgian Civil Code recognises five types of evidence: documentary evidence (certified documents, signed private deeds), oral evidence, presumption, confession, and statements made under oath. The law does not establish any categories of electronic evidence. Article 1322 of the Civil Code, and Article XII.15 of the Economic Law Code, reiterate the definition of electronic documents set out in the Law of 11 March 2003 on a number of legal aspects of information society services.		✓
Bulgaria	The assessment of the authenticity or reliability of evidence is made under articles 193 and 194 of the Civil Procedure Code.		✓
Czech Republic	The use of electronic evidence is not expressly regulated in the Czech civil law or in the administrative branch. Act N° 300/2008 Coll. on Electronic acts and on Authorized Conversion of Documents provides provisions on the authorized conversion of documents. Written original documents can be converted by means of authorized conversion to a digital version and vice versa. Converted documents are provided with an authentication clause that certifies the unity of input and output documents. As a result, it is possible to submit written evidence in electronic form and vice versa. Act N°300/2008 Coll. also states that a document created by means of conversion has the same legal effects as a certified copy of the	✓	

	original document.		
Denmark	There is no classification of evidence.		✓
Estonia	All evidence is presumed reliable, except if the opposing party challenges the evidence. If the opposing party objects, the submitting party should submit metadata or seek a court order to obtain metadata.	✓	
Finland	The categories of evidence in accordance with the Code of Judicial Procedure are: (i) hearing of a party for probative purposes, (ii) witnesses, (iii) expert witnesses, (iv) documents and (v) judicial inspection of an object. Electronic evidence is considered to be a document when a question concerns the content. In other cases, electronic evidence can be the object of judicial inspection.		✓
France	French law draws a distinction between written evidence, testimonial evidence, a presumption, an admission and an oath. Written evidence is distinguished as to whether it takes the form of a private document or an authentic instrument, as defined by article 1317 of the Civil Code. The instrument's probative force is particularly strong, as it is considered authoritative until proven otherwise. Electronic-based writing has the same value as paper-based writing, as provided for by article 1316-1 of the Civil Code. An authentic instrument may moreover be drawn up on an electronic medium under the terms of the second paragraph of Article 1317, as cited above. Not all forms of evidence have the same force, because writing takes precedence over testimonial evidence. An admission is a statement whereby a person acknowledges as true, and to be taken as proven in respect of him/her, a fact capable of having legal consequences for him/her. It may be judicial or extra-judicial. In the first instance, it is indivisible and constitutes conclusive evidence, since, under article 1356 of the Civil Code; it is deemed fully authentic proof against the person who made the admission. In the second instance, its probative force is left to the discretion of the court.		✓

Georgia	According to the Civil Procedural Code of Georgia, there are 5 types of evidence: parties' clarifications, written evidence, material evidence, witness testimony and the expert opinion. Provisions on electronic evidence are under the heading of written evidence. According to article 134 of the Code, an electronic document that is confirmed using an electronic signature as defined in the law of Georgia on Electronic Signature and Electronic Document should be regarded as evidence. According to article 3 of the law. The court has no right to dismiss evidence because it is provided in an electronic form.		✓
Germany	Section 371a para 1 ZPO holds that the rules concerning the evidentiary value of private records and documents shall be applied mutatis mutandis to private electronic documents bearing a qualified electronic signature. The appearance of authenticity of a declaration available in electronic form, as obtained from reviewing it pursuant to the Electronic Signature Act (Signaturgesetz), can be cast into doubt only by facts giving rise to serious doubts as to the declaration having been made by the holder of the signature key. If a qualified electronic signature is missing, the rules on visual evidence apply (Sect. 371 Para. 1 ZPO). If electronic documents are created in accordance with the requirements as to form (public electronic documents) by a public authority within the purview of its official responsibilities, or by a person or entity vested with public trust within the sphere of business assigned to him or it, section 317a para 3 states that the rules concerning the evidentiary value of public records and documents shall be applied mutatis mutandis. Where the document bears a qualified electronic signature of the public authority that has created it, it shall be presumed to be authentic. The same shall apply if an accredited service provider furnishes the document on behalf of the public authority that has created such a document. Where is it furnished on behalf of the person or entity vested with public trust that has created such a document with his qualified electronic signature pursuant to section 5 (5) of the	✓	

	Act on De-Mail, and the sender authentication identifies the public authority that has created the document, or the person or entity vested with public trust as the user of the De-Mail account, or the person or entity vested with public trust. Regarding public records or documents that have been transformed, using state-of-the-art technology, into electronic documents by a public authority, or a person or entity vested with public trust, and electronic documents created by a public authority within the purview of its official responsibilities, the rules concerning the evidentiary value of public records and documents apply where a confirmation is available that the electronic document is a true and correct copy of the original, both as an image and in terms of its substance. Where the document and the confirmation bear a qualified electronic signature, it is presumed to be authentic (section 371b ZPO).		
Greece	The Greek Civil Procedure Code does not contain special provisions regarding the use of electronic evidence. Article 339 of the Civil Procedure Code provides as follows: 'Means of evidence are the following: confession, autopsy, expertise, documents, examination of litigant parties, witnesses and judicial presumptions.' This means that electronic evidence fits into the evidential schema under the definition of documents. See the accompanying compilation of responses for more detail.		✓
Hungary	Article 166 (1) of the Civil Procedure Act provides that means of proof includes testimonies, expert opinions, inspections, documents and other physical evidence. In this list of examples, electronic evidence may also fit into the classification of object of inspection, electronic document or other physical evidence, but may also form an unspecified independent category.	✓	
Ireland	Irish law classifies evidence as oral testimony, real evidence and documentary evidence. Electronic data may be real evidence insofar as it is an object the existence of which or the character of which may be		✓

	relevant to the issue in suit. In this regard it is treated in the same manner as documents.		
Italy	The Italian system allows the parties to submit any document or other evidence in any possible form.		✓
Latvia	The categories of evidence are explanations of the parties and third persons, testimonies of witnesses, documentary evidence, demonstrative evidence, expert-examination and opinion of association of persons. Electronic evidence is likened to documentary evidence. The court assesses the admissibility of the evidence. Evidence submitted by the public authority is deemed as safe and credible. The court pays additional attention to evidence submitted by private persons if there is a reason for the court to doubt it.		✓
Lithuania	See the accompanying compilation of responses.		✓
Malta	Evidence can either be verbal or documentary evidence: Code of Organization and Civil Procedure – Chapter 12 of the Laws of Malta. Electronic evidence falls under documentary evidence.		✓
Montenegro	There is no classification of evidence. All evidence has the same legal power. When it comes to public documents – that is a document issued in the prescribed form by a public authority within the limits of its competence – and the document issued in that form by an enterprise or another organization in the exercise of its public power prescribed by law, it is considered to be accurate, but it is possible to prove otherwise (Article 226 of Law on Civil Procedure). If a public document is submitted in electronic form the same shall apply to it.		✓
Norway	The Dispute Act classifies evidence in three categories: testimonies, expert evidence and real evidence. Electronic evidence is a form of real evidence. The classification only decides which set of procedural rules should be used when evidence is presented before the court, and does not contain any presumption of authenticity or reliability of the evidence. Norwegian law does not operate with		✓

	general rules of evidence. The authenticity and reliability of evidence is decided by the court on a case-by-case basis based on a free evaluation of the facts. There are no presumptions as to the reliability or authenticity of electronic evidence.		
Poland	There is no specific classification of electronic evidence. As an example of possible treatment one may point out that standard mail (from address user@domain) may be considered as anonymous communication. The indication of the name in the electronic address will probably not be considered as equivalent to signature. The same may apply to the indication of personal particulars in the message. The control over the access to an e-mail account by the user (whether shared with other persons) might also be taken into consideration.		✓
Portugal	Decree-Law 290-D/99, of 02-08 (amended and republished by Decree-Law 88/2009, of 09-04) regulates the legality, efficacy and probative value of electronic documents and digital signatures. Electronic forms and other electronic communications are considered electronic documents. Article 2(a) of the Decree-Law 290-D/99, of 2 August (amended and republished by Decree-Law 88/2009, of 9 April) provides that an electronic document is a document produced through the electronic processing of data.	✓	
Romania	Legal instruments or facts may be proven by means of written documents, witnesses, presumptions, testimonies by one of the parties, made willingly or during interrogation, by means of expert reports, material evidence, on-site investigation and any other means prescribed by law (article 250 of the New Code of Civil Procedure). As regards written evidence, the New Code of Civil Procedure has introduced rules concerning documents in computer-readable format (article 266 and articles 282-284) and in electronic format (article 267).	✓	
Russian Federation	Electronic evidence is not classified as separate evidence in the Russian legislation, and is reviewed as a	✓	

	document (documentary evidence) or physical evidence. According to Article 26.7 Part 2 of the RF CAO, the document may contain information recorded both in writing and in a different form. Such documents can include the materials obtained as a result of photography and filming, sound and video recordings, from information databases and data banks, and other media. In cases where the documents have the signs referred to in Article 26.6 of the RF CAO, such documents shall be recognized as physical evidence. Please see the response for a more detailed analysis of the position.		
Serbia	No response.		✓
Slovak Republic	The classification of evidence is listed in § 125 of the Code of Civil Procedure. Evidence is any mean by which the state of affairs can be established, mostly by deposition or testament of witness, expert opinion, statements and opinions of public authorities, natural or legal persons, written documentation, examination on site and interrogation of participants. There is no distinctive rule that applies to electronic evidence regarding its authenticity or reliability. General rules apply as for all written documents. The court rules on the fashion in which the evidence is to be carried out, unless it is provided for a specific purpose.		✓
Spain	All issues affecting electronic evidence are governed by general rules or dispositions established for classic or normal evidence. There are no specific or different rules to be applied to electronic evidence.		✓
Sweden	Swedish procedural law relies on the principles of free submission and free evaluation of evidence. These principles mean that anything that may be of value as evidence in a case may, in principle, be presented at the main hearing. Furthermore, evidence is not given a particular evidentiary value as such. The judge with regard to circumstances in the case in question assesses the evidentiary value.		✓

Switzerland	There is no classification of evidence. The principle of free assessment and evaluation of evidence applies (Article 157 CPC).		✓
Turkey	The types of the evidence are laid down in Civil Procedure Code numbered 6100. These are defines as documents and bills, commencement of evidence, oath, witness, expert, viewing and expert opinion. Electronic data is accepted as documents in accordance with article 199 of the same Code. In accordance with article 205, electronic data, which is drawn up by a secure electronic signature, are deemed as an electronic bill.		✓
Ukraine	No response.		✓
UK (England & Wales)	There are broadly two types of evidence: direct and indirect. The existence of a physical object is direct evidence; indirect evidence encompasses facts that can be inferred form the direct evidence. There is also a lawyerly definition as in 'real evidence'. This is defined as material evidence produced without human intervention. Electronic evidence falls into all of the above classifications. The general rules in terms of evidence is that the judge will admit almost any evidence, and it is for the parties to argue the weight that it should have attached to it.	✓	

Part D The admissibility and integrity of electronic evidence

Preamble

55. Many jurisdictions have provided for the admissibility of electronic evidence into legal proceedings. This issue has also been addressed regionally, such as the provision of article 5(2) of the European Union Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,[6] which provides that an electronic signature cannot be 'denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form'. Similarly the provision of article 9(1) of the European Union Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'),[7] provides that contracts shall not be deprived of legal effectiveness and validity on account of their having been made by electronic means. It is generally accepted that evidence in electronic format is admissible in legal proceedings. Rules might include:

(i) whether the evidence should be obtained in accordance with any technical guidance, (for instance, guidelines exist for criminal proceedings, and they can be useful for civil and administrative proceedings[8]), and

(ii) how the authenticity and reliability of electronic evidence is determined – that is, whether there are any agreed guidelines laid down that helps a judge determine the authenticity of electronic evidence, and if there is any presumption regarding the 'reliability' of electronic evidence.

56. Question 10
Is a party wishing to submit electronic evidence in civil or administrative proceedings required to have obtained it using a specific procedure, as required by law or otherwise?

Analysis of responses to question 10

57. No member state has a legal requirement to obtain electronic evidence using a specific procedure.

58. Aside from the requirement of obtaining evidence by means of a special procedure, in Croatia, the Electronic Document Act deals with copies of electronic documents (presumably the contents of electronic documents, because there is no reference to the metadata) printed on paper. In England & Wales, civil procedural rules apply to all civil proceedings. In Greece, the provisions of Presidential Decree 150/2013 set out the principles and terms that a party is required to abide when submitting electronic evidence.

[6] OJ L 13, 19.1.2000, p.12. The Directive will be repealed by Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L257, 28.8.2014, pp. 73–114.

[7] OJ L 178, 17.7.2000, pp. 0001 – 0016.

[8] For example: *Guidelines for Best Practice in the Forensic Examination of Digital Technology*, Version 6 (20 April 2009), European Network of Forensic Science Institutes, Forensic Information Technology Working Group, available at http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf; UK Association of Chief Police Officers 'Good Practice Guide for Digital Evidence', Version 5 (October 2011), available at http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf.

The first article of the decree requires the electronic evidence in civil proceeding is to be accompanied by an advanced electronic signature. In the Russian Federation, electronic evidence must comply with the requirements of the relevant federal laws, including the Civil Code, and Federal Law dated 6 April 2011 No. 63-FZ on Electronic Signature.

59. Question 11
If electronic evidence is not obtained in accordance with any standard or special procedure, will the court take this into account in deciding whether to admit the evidence?

Analysis of responses to question 11

60. In general, the court will evaluate the evidence before it in the normal course of judicial proceedings, taking into account all of the technical evidence made available. In some jurisdictions, the judge will decide what evidence to accept and what evidence to have tested for authenticity.

61. In Greece, it depends on the facts of each case. Although there is no specific provision in Presidential Decree 150/2013, when considering an analogous interpretation of other civil code procedures, namely an private document – where electronic evidence is not obtained in accordance with any standard or special procedure, it lacks the evidential power of a private document and can be regarded as a document that does not contain all the necessary perquisites as required by law, and can only be freely estimated by the judge as evidence that does not conform to the requirements for adducing private documents.

61. Question 12
If not already mentioned elsewhere in your response, are there any technical guidelines or best practices that have been published in your country that describe how electronic evidence can be obtained while maintaining its integrity?

Analysis of responses to question 12

63. There have been guidelines produced in Poland (in Polish only – see the accompanying compilation of responses for more detail), but it is not clear if the guidelines refer to civil proceedings or criminal proceedings. There are guidelines in England & Wales in respect of criminal cases, but not civil proceedings, as noted in the questionnaire.

64. In Belgium, there are presumptions relating to the use of an advanced electronic signature. In Germany, there is a limited presumption regarding integrity where an individual has registered securely for a ‘De-Mail’ account that is assigned solely to that individual (section 4 (1), second sentence, of the Act on De-Mail). The appearance of authenticity attendant on an electronic message sent from a ‘De-Mail’ account, resulting from the verification of the sender authentication pursuant to section 5(5) of the Act on De-Mail, will be called into question only by facts giving rise to serious doubts as to the message with that content having been sent by that person (section 371a Para 2 Code of Civil Procedure).

65. In Montenegro, the Law on Electronic Signature provides for the creation of a set of rules relating to advanced electronic signatures, which, if followed, provides for a presumption of reliability.

66. Question 13
Do the rules on admissibility of electronic evidence vary according to the complexity or simplicity of the evidence, and if so, how?

Analysis of responses to question 13

67. The rules on the admissibility of electronic evidence tend not to vary according to the complexity or simplicity of the evidence. The amount of evidence to demonstrate the authenticity of digital data may alter, depending on the complexity of the evidence. In Belgium and Spain, the use of an advanced electronic signature attached or affixed to digital data will affect the ease of demonstrating authenticity.

Table 4

Responses to questions 10 – 13

	10		11		12		13	
	Yes	No	Yes	No	Yes	No	Yes	No
Andorra		✓		✓		✓		✓
Armenia		✓		✓		✓		✓
Belgium		✓		✓		✓		✓
Bulgaria		✓		✓		✓		✓
Croatia	✓		✓			✓		✓
Czech Republic		✓		✓		✓		✓
Denmark		✓		✓		✓		✓
Estonia		✓		✓		✓		✓
Finland		✓		✓		✓		✓
France		✓		✓				✓
Georgia		✓		✓		✓		✓
Greece		✓	✓			✓		✓
Germany		✓		✓		✓		✓
Hungary		✓		✓		✓		✓
Ireland		✓		✓		✓		✓
Latvia		✓		✓		✓		✓
Lithuania		✓		✓		✓		✓
Malta		✓		✓		✓		✓
Montenegro		✓		✓		✓		✓
Poland		✓		✓	✓			✓
Portugal		✓		✓		✓		✓
Romania		✓		✓				✓
Russian Federation		✓		✓		✓		✓
Serbia		✓		✓		✓		✓
Slovak Republic		✓		✓		✓		✓
Spain		✓		✓		✓		✓
Sweden		✓		✓		✓		✓
Switzerland		✓		✓		✓		✓
Turkey		✓		✓		✓		✓
Ukraine		✓		✓		✓		✓
UK (England & Wales)		✓		✓		✓		✓

Part E The archiving of evidence after trial

Preamble

68. Electronic evidence needs to be treated differently than paper files and case exhibits. By printing electronic documents, the relevant metadata that goes to prove the authenticity of the document is lost. This means that is it necessary to retain electronic data in its original form for as long as a paper case file would be retained. To this extent, it is necessary for lawyers and court administrators to provide for the confidentiality and security of such data, including the retention of secure back-up copies should one of the means of storage fail.

69. The Council of Bars and Law Societies of Europe (CCBE) have produced a set of guidelines dealing specifically with 'cloud computing', which is tangential to this study, but there is no other guidance provided by the CCBE that directly covers this topic.[9]

70. Question 14

What are the norms or professional conduct, if any, relating to the duty and requirements for the storage and preservation of electronic evidence?

In replying to this question, please cover the following discrete areas:

Archiving by lawyers

Archiving by the courts

Requirements to provide for the security of evidence after a trial

Analysis of responses to question 14

71. There is significant variation in the responses to question 14. The wide variety of responses illustrate that there appears to be a high degree of uncertainty about the provisions relating to archiving, and even more worrying, of the security that should be attached to electronic documents. To illustrate one jurisdiction, that of England & Wales (chosen because Stephen Mason practices in this jurisdiction), the position is, in more detail, as follows:

Archiving by lawyers

There is a duty to preserve evidence for as long as the court proceedings are live and any chance of appeal has passed.

In general terms, historically solicitors were responsible for the retention of client files (and therefore evidence adduced at trial). Once a trial ended, the barrister, if a barrister is engaged, will return the files to the solicitor. However, the digital age means this arrangement is now more complex, because the barrister will be in possession of electronic copies of the evidence and instructions, unless they make the decision to expunge all evidence of such data from their computers or servers. In practice, barristers will retain much of the evidence in electronic format.

[9] CCBE guidelines on the use of cloud computing services by lawyers, available at http://www.ccbe.eu/.

The Law Society of England & Wales and the Bar of England & Wales provide separate advice in relation to the retention of records – and by extension, the retention of evidence after trial. A text covers this topic,[10] and there are a number of practice guides: *Information security* (11 October 2011),[11] *File retention: trusts* (6 October 2011),[12] and *File retention: wills and probate* (6 October 2011).[13]

There is no specific advice regarding the retention of evidence after trial, but reference is made by the Law Society of England & Wales to the relevant provisions of the Limitation Act 1980, Value Added Tax Act 1994, Data Protection Act 1998 and the Money Laundering Regulations 2007 (2007 SI 2157). Generally, a solicitor will mark a file with a review period, and send the file to the partner responsible for a decision at the end of the period. In practice, most partners do not have the time to conduct such a review, and the general practice is to store physical files and their contents forever.

The Bar of England & Wales has provided the following guidance, which touches upon the topic: *Guidelines on Information Security*[14] and *Email Guidelines for the Bar*.[15] For those barristers that are qualified to provide legal advice and representation direct to the public, the *Public Access Guidance for Barristers* (January 2014) includes advice on this topic.[16]

Archiving by the courts

There is a duty to preserve the court papers for the current year plus between 7 and 12 years. It will depend on the jurisdiction. However exhibits are generally returned prior to that time or held depending on the nature of the evidence and the scope for further action.

No detailed information is available relating to this issue.

Requirements to provide for the security of evidence after a trial

The provisions of the Data Protection Act 1998 apply to all lawyers, so it is arguable that lawyers are required to provide for the security of electronic data, regardless of any professional rules or guidelines.

[10] Andrew Hopper QC, Cartwright Black and Iain Miller, gen eds, *Cordery on Legal Services* (LexisNexis Butterworths) looseleaf.

[11] http://www.lawsociety.org.uk/advice/practice-notes/information-security/.

[12] http://www.lawsociety.org.uk/advice/practice-notes/file-retention-trusts/.

[13] http://www.lawsociety.org.uk/advice/practice-notes/file-retention-wills-probate/.

[14] http://www.barcouncil.org.uk/for-the-bar/professional-practice-and-ethics/it-panel-articles/guidelines-on-information-security/.

[15] http://www.barcouncil.org.uk/for-the-bar/professional-practice-and-ethics/it-panel-articles/email-guidelines-for-the-bar/.

[16] https://www.barstandardsboard.org.uk/media/1580337/public_access_guidance_for_barristers_-_jan_2014.pdf.

The Law Society *Information security* (11 October 2011)[17] is a very wide-ranging commentary with little of substance regarding the security of electronic data. Solicitors are directed to a particular text: Keith Mathieson, *Privacy Law Handbook* (Law Society Publishing, 2010).

In addition, the Solicitors Regulation Authority *Code of Conduct*[18] sets out a number of mandatory Principles that a solicitor must follow. Chapter 7, 'Management of your business', sets out a number of outcomes that every solicitor must adhere to. There are a series of 'Indicative behaviours' that, if followed, might show that the solicitor has achieved the outcomes and therefore complied with the Principles. The following are relevant for the purposes of providing for the security of electronic data:

> IB(7.1)
> safekeeping of documents and assets entrusted to the firm;
>
> IB(7.3)
> identifying and monitoring financial, operational and business continuity risks including complaints, credit risks and exposure, claims under legislation relating to matters such as data protection, IT failures and abuses, and damage to offices;

The Bar of England & Wales provides guidance regarding the security of electronic data in *Guidelines on Information Security*.[19] However, the guidelines do not form part of the Code of Conduct, and following them does not necessarily provide a defence to complaints of misconduct or of inadequate professional service. It is the individual responsibility of the barrister to preserve the confidentiality their client's affairs.

72. The response from the Ministry of Justice of the UK illustrates that there is some knowledge of archiving and security, but the full ramifications have yet to be widely understood regarding data in electronic format.

[17] http://www.lawsociety.org.uk/advice/practice-notes/information-security/.

[18] http://www.sra.org.uk/solicitors/handbook/code/content.page.

[19] http://www.barcouncil.org.uk/for-the-bar/professional-practice-and-ethics/it-panel-articles/guidelines-on-information-security/, pp. 18 – 27.

Table 5

Responses to question 14

	Response
Andorra	Article 60 of the Qualified Law on Justice of 3 September 1993, as amended at the end of 2014, provides that responsibility for the preservation and storage of all documents and archives, and for the conservation of property and objects included in or assigned to case files, lie with the registrar of each court.
Armenia	There is no any legal regulation or any provisions of professional conduct on the storage and preservation of electronic evidence for courts or for lawyers. Article 7 of Law on Electronic Document and Electronic Signature provides as follows: Article 7. Storage of electronic documents An electronic document is considered to be duly stored, if it has not undergone any changes since it was sent for storage, or it has changed due to its storage requirement, and it is possible to restore the electronic document in the form it was before storage. The electronic document verified by an electronic signature is considered duly stored if its signature-verification data have also been kept. The owners of information systems provide the protection of electronic documents stored in their information systems.
Belgium	Belgian law does not yet include regulations governing electronic archiving. **Lawyers** Article 2276bis of the Civil Code governs archiving by lawyers, which provides as follows: '§1.Lawyers are discharged of their professional responsibility and the conservation of documents five years after the completion of their task. This time-limit is not applicable if the lawyer has been expressly designated as the custodian of specific documents.' **The courts** The Law of 24 June 1955 on archives [*Belgian Official Gazette*, 12 August 1955 and Royal decree of 18 August 2010 implementing Articles 1, 5 and 6bis of the law of 24 June 1955 on archives (*Belgian Official Gazette*, 23 September 2010, Addendum, *Belgian Official Gazette*, 22 October 2010)] governs the archiving by court registrars in particular.
Czech Republic	**Lawyers** Advocates are bound to store documentation and client files for the period of 5 years from the day the representation ended (article 3 of the Resolution of the Board of the Czech Bar Association N°9/1991). This rule also applies to electronic evidence. There are no special rules imposed on how to store electronic evidence. **The courts** Evidence received in electronic form is archived on portable discs and within the information system of the courts. In other cases, e.g. when the evidence is the content of an e-mail communication or an up-to-date view of a social networking page, the evidence is taken as follows: the page is observed during the hearing by the judge who then takes a print screen of the displayed content. The print screen will be then printed out on paper and stored in the case file. **Security of evidence after a trial** The general rules on the storage of evidence apply for evidence archived on portable discs; the storage within the information system of the courts is regulated by internal

	regulation of the Ministry of Justice.
Denmark	There are no such norms, especially for electronic evidence.
Estonia	E-mail/web page metadata is normally converted into PDF and/or printed and stored as such. Digital signature files are stored in the court database (e.g. e-curia); printouts are stored in printed form.
Finland	Courts are obliged to file documents, visual or verbal/lingual material, including electronic documents according to the act 831/1994 ('Archive Act', no translation available). Material has to be preserved in a way that it will not be destroyed, damaged or used in an inappropriate manner. The Code of Conduct for Lawyers prepared by the Finnish Bar Association provides for the security of information systems in clause 11.6: 'A lawyer shall ensure that the security of information systems in the office does not allow third parties to view client information without authorisation.' The Finnish Bar Association has also given an order about information security and a manual supporting the position (no translations available). The order includes, for example, rules for the securing of the computer and other devices (passwords, virus protection, protection of movable computer and wi fi etc.) and rules of obligation to look after information security when making a contract, for example with outside IT-company and archive security rules.
France	In general, as regards evidence, the principle of equivalence between electronic-based writing and paper-based writing follows from compliance with the storage conditions necessary to preserve its integrity (article 1316-1 of the Civil Code). Similarly, an authentic instrument may be drawn up on an electronic medium only if it is stored under conditions that preserve its integrity and legibility (article 1317 of the Civil Code). A notarised instrument drawn up on an electronic medium is accordingly registered in a central minutes-record, with a view to its conservation, as soon as it has been established by the attesting notary, who retains exclusive access to the instrument (article 28 of the Decree of 26 November 1971, as amended). As regards the procedure, technical processes' ability to guarantee the conservation of transmissions performed is also a condition for the use of electronic communications (article 748-6 of the CCP). With regard to bailiffs, the legislation (article 26 of the decree of 29 February 1956, as amended by the decree of 10 August 2005) requires that original instruments drawn up on an electronic medium must be established by means of a processing, storage and information transmission system approved by the National Chamber of Bailiffs and guaranteeing the integrity and confidentiality of their content. **Lawyers** Original documents are returned to clients after the proceedings. Article 2225 of the Civil Code provides for a limitation period of five years during which a client may initiate proceedings against his/her lawyer in the event of an error. This five-year limitation period is a relatively recent legal provision, which was introduced by a law of 17 June 2008. Lawyers are obliged to keep a copy of documents, including those in electronic form, for a minimum of five years following the proceedings. However, it should be noted that, in practice, lawyers keep copies thereof for a longer period as a precautionary measure. A number of cases have set precedents in this matter, especially with regard to determination of the moment when the period of five years should begin to run. **Court registries** In accordance with the rules applicable to public administrative authorities, any digital archiving performed by courts should comply with the OAIS model (Reference Model for an Open Archival Information System, published by ISO under reference ISO 14721:2003).

Georgia	There are no special rules on this matter.
Germany	**Lawyers** The norm relating to the duty and requirements for the storage and preservation of files by lawyers is mainly § 50 of the Federal Lawyers' Act (Bundesrechtsanwaltsordnung, BRAO). The norm has the following content: BRAO § 50 The Rechtanwalt's files (1) A Rechtsanwalt must be in a position to give an orderly account of his/her professional work. This must be done by creating files. (2) The Rechtsanwalt must keep the files for five years after bringing a case to a conclusion. However this duty shall lapse, even before this period has ended, if the Rechtsanwalt has requested the client to take the files and the client has not met this request within six months of receiving it. (3) A Rechtsanwalt may refuse to surrender the files to the client until the Rechtanwalt's fees and disbursements have been paid. This shall not be the case in as far as it would be unreasonable in the circumstances to withhold the files or individual documents. (4) Files in the meaning of paras 2 and 3 of this provision are only the documents that the Rechtsanwalt has received for or on behalf of the client on grounds of his/her professional practice, but not the correspondence between the Rechtsanwalt and the client nor documents where the client has already received the original or a copy. (5) Para. 4 shall apply accordingly in as far as the Rechtsanwalt uses electronic data processing in order to keep files. Apart from this norm the Rechtsanwalt has the basic duty to observe professional secrecy, § 43a para 2 BRAO. **The courts and requirements to provide for the security of evidence after a trial** There are no general rules on the standards of archiving by the courts in the code of civil procedure. The rules on archiving are left to the Länder, which have each developed their own rules ("Aktenordnung"). Additionally, Section 298a ZPO in the current version holds: (1) The court records of the dispute may be kept as electronic files. The Federal Government and the Land governments determine, by statutory instrument, for their sphere of responsibility the time onwards from which electronic files are to be kept, as well as the framework conditions in organisational and technical terms governing the creation, administration, and storage of the electronic files. The Land governments may confer, by statutory instrument, the corresponding authorisation upon the Land departments of justice. (2) Any documents and other records submitted on paper are to be changed to electronic format by way of replacing the original. Should the documents and records still be needed in paper format, they are to be stored at least until the proceedings have been concluded as res judicata. (3) The electronic document must include the note as to when and who changed the documents to electronic format.
Greece	**Lawyers** Lawyers bear some obligations that relate to their clients and the proceedings in a court. Once litigation has begun (even if the case is dismissed and comes to an end, no matter what the result), the lawyers are obliged to retain all relevant documents for at least five years (article 37 §8 Code of Conduct of Lawyers); the same obligation exists for the court file records, which are also retained for a maximum of five years and then destroyed. Failure to comply with these provisions may mean the violating lawyer faces disciplinary action. In cases of a serious violation, criminal sanctions can

	also be imposed. It has been held that once a lawyer adduces evidence and documents in court, he has no longer ownership over them; this means that he cannot destroy them deliberately or alter them by any means, because he will be liable and prosecuted for the penal offense of defalcation of documents (article 222 Penal Code) or forgery (article 216 Penal Code) respectively, for which see: Supreme Court (5th Penal Chamber) 566/2006 (AP (penal chamber) 566/2006). **The courts** According to the provisions of article 6 of the Presidential decree 150/2013 relating to electronic procedure before civil courts, the courts are obliged to obtain and preserve an electronic file of all pleadings and relevant documents (evidence and procedural documents) that were adduced and any other electronic document relevant to the case. All preserved electronic archives should meet all the requirements and terms of security and guarantee the integrity, the authenticity, the confidentiality and the quality of the documents and the data that are included in them.
Hungary	**Lawyers** Obligations of confidentiality apply to of law firms and their employees, attorney bodies and their officials and employees, as well as natural and legal persons responsible for the storage, archiving, preservation and processing of the data incorporated in electronic or paper documents containing data classified as client-attorney privileged information: paragraph (4) of Article 8 of Act XI of 1998 on Attorneys at Law. Pursuant to article 2(1) of Decree 114/2007 (29 December) of the Minister of Economy and Transport on the Rules of Digital Archiving, the party obliged to preserve documents is required to ensure that electronic documents are preserved in a manner that excludes the possibility of subsequent modification and protects these documents from being deleted, destroyed, accidentally destroyed, damaged, as well as against unauthorised access. **The courts** Article 6(5) of Directive 17/2014 (23 December) on standard rules for documents managed by courts issued by the National Office for the Judiciary requires the court to preserve electronic documents, documents, as well as electronically archived case documents and documents compiled during the course of its regular operation in electronic archives. Article 195(1) provides that court documents must be safeguarded until the expiry of the safekeeping period or up to the date they are handed over to the competent archives.
Ireland	**Solicitors** In civil proceedings, the original evidence is placed on the court file. Solicitors retain copies of documents admitted in evidence on their files. The Law Society of Ireland which is the professional body governing solicitors in Ireland has issued a *Guide to Professional Conduct of Solicitors in Ireland Law Society* (2nd Edition 2002) which states at 9.13: “In order to protect the interests of clients who may be sued by third parties and also to protect the interests of the solicitors’ firm which may be sued by former clients or by third parties, a solicitor should ensure that all files, documents and other records are retained for appropriate periods.” The reference to ‘appropriate periods’ is to appropriate periods of limitation for the issue of proceedings that is typically 6 years but may be up to 12 years for contracts under seal. The Technology Committee of the Law Society of Ireland has issued a Practice Note which requires Solicitors to retain documents relating to litigation for at least 6 years being the period within which clients can bring proceedings relating to the

	solicitor/client contract and the availability of the file for the solicitor's professional indemnity insurers. The Practice Note provides that: "[w]here documentation is properly stored in an electronic format (and subject to any statutory or regulatory limitations on storage or retention in electronic format), the paper version (if one existed) need not be retained. The three key issues affecting electronic storage are: permanency or durability of the format; accessibility of the format; security of the format." Where material is being stored electronically the Practice Note requires that it should be in an open format so that its future availability and accessibility will not be compromised. **Barristers** When Barristers are instructed in contentious matters the relevant documentation is included in the brief prepared for the trial or appeal. Briefs are returned to the instructing solicitor at the end of the trial or appeal. When Barristers instructed in advisory matters will typically return the documents that are annexed to the Case for Counsel to the instructing solicitor with the Opinion or advices as the case may be. **The courts** After the conclusion of a civil procedure, the paper file containing the pleadings and certain other documents some of which have the character of evidence, such as sworn affidavits, is retained in the custody of the Courts Service, which is an independent corporate organisation established by the Courts Service Act, 1998 which, amongst other things, manages the courts and provides support services for judges. The exhibits that have been adduced in evidence are returned to the party by whom the evidence has been adduced. Similarly in criminal procedure the evidence such as the disc or tape containing video images is returned to the prosecuting authority or the defendant as the case may be. It might be noted that the new Court of Appeal has a (publicly funded) digital project underway to facilitate e-filing which could mean that much information on a case, such as pleadings, could be made available in electronic form. Court files are subject to the provisions of the National Archives Act 1986 being classified as "Departmental Records" by Sub-s 1(2)(b) of the Act. Section 7 of the National Archives Act, 1986 deals with retention and disposal of Departmental records. Sub-s 7(1) requires that Departmental records that have not been transferred to the National Archives in accordance with s. 8 or are disposed of under Sub-s 7 (5) must be retained and preserved in the Department of State in which they were made or are held. Sub-s 7(2) permits the Director or "the designated officer") to authorise the disposal of the Departmental records in certain circumstances such as on the written application of the particular Department of State where the records are not required in connection with the administration of that Department; where the Director of the National Archives or the designated officer is satisfied that the records do not warrant preservation by the National Archives. In the case of Court records, Sub-s 7 (4)(c) provides that the Chief Justice, in the case of records of the Supreme Court, or the President of the High Court, in the case of records of the High Court, has consented to the making of the authorisation.
Lithuania	There are no special rules concerning the duty and requirements for storage and preservation of electronic evidence. Electronic evidence submitted via the Lithuanian Court Information System is stored by the courts in accordance with Regulation No 13P-74-(7.1.2) of 20 June 2013 of the Council of Judiciary covering the rules that apply to the processing, archiving and storage of electronic data related to legal proceedings using information and communication technologies.
Latvia	There are no special regulations developed for civil and administrative courts in

	relation to the storage of electronic evidence that are present in the materials of the case file. Electronic evidence shall be stored in the matter, upon recording them to CD disk or other data carrier, such as a flash memory. The procedure is determined by Cabinet Regulation No. 748 'Regulations Regarding Records and Archives Management', adopted on 6 November 2012. This Regulation determines that file readability shall be verified for electronic documents. Depending on the type of a data carrier, the temperature for storage may differ.
Malta	**Lawyers** In article 101A of the Constitution of Malta, the Commission for the Administration of Justice set out the Code of Ethics and Conduct for Advocates. Rule 6 under Chapter III of the Code of Ethics provides that 'On termination of the brief an advocate should, subject to any privilege and/or right of retention, deliver to the client all papers and property to which the client is entitled and account for all funds of the client then held by the advocate'. Chapter VI of the Code of Ethics deals with confidentiality. **The courts** There is a duty to preserve the records of the courts in terms of the National Archives Act (Chapter 477 of the Laws of Malta) as such records are considered to be public records and archives.
Montenegro	The archiving of electronic evidence as electronic documents is regulated by article 21 of the Law on electronic document, which provides: Legal persons, natural persons and competent bodies are obliged to store the electronic documents originally in the information systems or on the media which provide the continuity of the electronic record for a determined storage time, in accordance with the Law, i.e. a legal affair. The electronic documents referred to in paragraph 1 of this Article shall be stored in electronic archive. The electronic archives must ensure that: 1) the electronic documents are stored in the form in which they have been created, dispatched, received and stored and which does not change materially the content of the documents; 2) the electronic documents are available in a readable form during the whole storage time to persons who have the right to access those documents; 3) data on electronic signatures with which the electronic documents have been signed, as well as data for verification of those signatures are stored; 4) the electronic signatures are stored in a form and with the use of technology and procedures which, along with the incorporated electronic signatures, provide a reasonable guaranty for their authenticity and integrity during the entire storage time and that they cannot be changed or removed without authorization within the time period stipulated by the Law and a legal affair; 5) it is possible to determine authentically for every electronic document the origin, creator, time, manner and form in which it has been received into the system for storage; 6) the procedures of maintenance and replacement of media for storage of the electronic document do not impair the integrity and inviolability of the electronic documents. The protection of electronic documents is set out in article 24: Appropriate technological procedures and equipment, which ensure the protection of electronic document, must be applied in the documentation cycle of the electronic document, in accordance with the Law. In procedures in which information equipment and communication system of the

	information intermediary are used, the information intermediary shall ensure the protection of the electronic documents.
Norway	Evidence remains stored at Lovisa after the end of the trial. Only court officials with personal passwords can obtain access to Lovisa. All paper copies of evidence are destroyed after the trial. **Lawyers** There is no general law regulating lawyers' archiving of legal documents. The procedures regulating lawyers' archives are covered by various items of specific legislation (privacy laws and anti-money laundering laws being the most important) and standards of professional conduct. Act of 14 April 2000 no. 31 relating to the processing of personal data (Personal Data Act) requires lawyers to put in place adequate data security measures to protect sensitive client information. The adequacy of the security measures have to be reassessed continuously and the lawyer is obliged to take necessary measures to address identified weaknesses. At the end of a case, professional standards require that the lawyer should go through the documentation amassed and decide what should be stored, destroyed or returned to the client. Client archives are generally stored for 10 years. This is done to document how the case was processed, in case the client later claims damages for inadequate legal advice. After 10 years original documents are returned to the owner and the rest of the client file destroyed. Professional standards dictate that lawyers archive the original documents. How electronic evidence is stored will, however, depend on whether the lawyer has a physical or electronic archive. Whether the lawyer archives the version of the electronic evidence containing the complete metadata also depends on the source of the evidence. The client often provides the evidence. The client will occasionally attach the electronic evidence, but in other cases the evidence might first be printed and then scanned or downloaded to another format before being sent to the lawyer. In other cases the lawyer will discover the piece of electronic evidence independently and archive it directly.
Poland	There are no common legal rules applicable to electronic evidence, including its securing and conservation.
Portugal	The rules are the same as the that apply to documentary evidence, that is to say the Regulation for the Maintenance of the Archive of the Courts of Law and of the Administrative and Tax Courts (approved by Order 368/2013, of 24 December), which are applied to documents produced and received in the scope of their duties and powers by the courts of law and by the administrative and tax courts (in particular, article 12).
Romania	**Lawyers** In accordance with the relevant provisions of Decision No. 64/03.12.2011 of the National Union of Bar Associations of Romania concerning the adoption of conditions of service governing the legal profession, lawyers are bound to record any instruments drawn up, and to store them in the professional archives, in the order in which they were drawn up. Within not more than three days from the date on which the instruments were drawn up, on pain of non-enforceability against third parties, the lawyer is required to record the operation in the electronic register of instruments drawn up by lawyers. Lawyers are bound to keep written proof of any operations carried out pursuant to or in connection with a fiduciary mandate. Where the client requests the original of these documents, the lawyer has the right to keep paper or electronic copies. **The courts** In accordance with the relevant provisions of Decision No. 387/22.09.2005 approving the Rules of Procedure of Courts, presidents and vice-presidents of courts and chief registrars organise and supervise the electronic archiving of case files at court level,

	respectively. Archivists and registrars have responsibilities with regard to the electronic archiving of case files, where practicable, and the IT staff are responsible for operating the electronic archiving system; they draw up the documents required in order to obtain electronic signatures for the courts and officers of the court, the certificates provided for in Law No. 455/2001 on electronic signature.
Russian Federation	Evidence in electronic format is subject to the general legal requirements to ensuring safety. In accordance with article 26.7 of the Code of Administrative Offences of the Russian Federation (RF CAO), the judge, agency or an official in charge of the administrative proceedings is required to take the necessary measures to ensure the safety of the documents before the resolution of the case on the merits, as well as to make decisions at the end of the proceedings. In accordance with article 26.6 Part 3 of the RF CAO, the judge, agency or an official in charge of the administrative proceedings is required to take the necessary measures to ensure the safety of the material evidence before the resolution of the case on the merits, as well as to make decisions at the end of the proceedings. Evidence shall be stored in accordance with the orders of the Judicial Department at the Supreme Court of the Russian Federation December dated December 15, 2004 No. 161 On Approval of the Instruction on Judicial Proceedings before the Supreme Courts of Republics, Territorial and Regional Courts, Courts of Federal Cities, Courts of Autonomous Region and Autonomous Territory and dated April 29, 2003 No. 36 On approval of Instructions on Judicial Proceedings before the District Court.
Serbia	The National Assembly adopted a Law on electronic document, which covers the storage of electronic documents. In accordance with the provisions of this Law, legal entities and natural persons and authorities are obliged to preserve and archive electronic documents in the information system or on media that is sufficiently durable for the storage time set out, and in accordance with the law regulating the archives, the law governing electronic signature and regulations on office operations. Legal entities and natural persons can undertake the storage of electronic documents for a legal entity that is required to undertake these tasks in accordance with the law. The legal entity entrusted with preserving electronic documents is not responsible for the content of the original documents. **Protection of electronic documents** Appropriate technological procedures and equipment must be used for electronic documents that ensure the protection of those documents, in accordance with the law regulating the archives, regulations on office operations and international standards in the field of document management.
Slovak Republic	Ordinance No. 543/2005 Col. (Administrative and Office Order of Courts (District, Regional and Martial) governs the rules for the archiving and storage of judicial files. The same rules cover filings lodged via electronic means (electronic evidence included). As a general rule, a file in a civil matter is subject to archiving for a 20-year period after the proceedings are finally closed. Thereafter, the file is either scheduled for destruction or forwarded to the National Archive if deemed relevant. In case of filings lodged electronically with a certified electronic signature, e-mails are stored on court servers alongside all lodged electronic documentation (i.e. motions, evidence etc.) since the implementation of electronic filing system.
Spain	There are no different rules governing the storage and preservation of electronic evidence generally speaking. It depends on specific sectors or specific evidence. The general rule under article 148 LEC 1/2000 is that clerks are responsible for the storage and preservation of proceedings archived by courts. The European Court of Justice judgment dated 8 April 2014 under reference numbers C-293/2012 and C-594/2012, for a preliminary ruling affecting the legality of Directive 2006/24/CE may affect the position. It is not as clear that the Spanish implementation Law 25/2007, of

	18 October 2007, on keeping data related to electronic communications and public communication networks will be affected.
Sweden	The courts – as well as other authorities – are obliged to archive public documents. Documents may be sorted out after a period of time, e.g. recordings from a hearing in court may be deleted six weeks after the judgment has become final. There are no particular rules governing electronic documents. The legislation is technology neutral. Pursuant to the Code of Professional Conduct for Members of the Swedish Bar Association, a Member of the Bar Association is obliged to archive all relevant documents filed in connection with a mandate either in original or as copies. However, this does not apply to duplicates, printed matter or similar material, which without difficulty can be obtained elsewhere. The archival period is ten years or more, depending on the nature of the mandate. Documents other than original documents that belong to the client may be archived in either photographic or electronic form.
Switzerland	**Lawyers** There are several laws providing a duty for storage and preservation of evidence in general, including electronic data and files, which have to be met by lawyers. Regulations on professional conduct include provisions for the length of retention of documents, including article 11 of the Cantonal Lawyer Act of Berne, which provides that lawyers have to preserve case documents for ten years. According to some doctrines, such a rule (ten years preservation) should be applicable to lawyers from other cantons as well. In connection with the period to preserve documents, there are no special rules referring to electronic data and files. **Federal courts** Different rules apply to federal courts than to cantonal courts. The Federal Supreme Court, the Federal Criminal Court and the Federal Administrative Court have their own regulations regarding the archiving of documents including electronic data and files (there are no special rules for them). The Federal Supreme Court and the Federal Administrative Court preserve only trial records that are directly connected to the activities of the courts (Article 3 para 1 of the Ordinance of the Federal Supreme Court to the Federal Act on Archiving and Article 3 para 1 of the Regulations on Archiving by the Federal Administrative Court; e.g. written submissions, judgements, correspondence, protocols etc.). They retain them permanently (Article 3 para 1 of the Ordinance of the Federal Supreme Court and Article 3 para 1 of the Regulations on Archiving by the Federal Administrative Court). However, these courts in principle do not retain further documents, such as means of evidence etc. Such documents will be returned to the editor (Article 3 para 2 of the Ordinance of the Federal Supreme Court and Article 3 para 2 of the Regulations on Archiving by the Federal Administrative Court). In accordance with the provisions of to article 39 para 1 of the Federal Act on the Organisation of the Prosecuting Authorities, the Swiss Criminal Procedure Code applies to the Federal Criminal Court as well as to cantonal courts. Article 103 of the Swiss Criminal Procedure Code provides for the preservation of case documents in criminal matters. Article 3 para 1 of the Regulations on Archiving by the Federal Criminal Court requires the court to retain the trial records permanently. Original documents have to be returned to the persons entitled thereto as soon as the criminal case has been decided by a final judgment (article 103 para 2 Swiss Criminal Procedure Code). **Cantonal Courts** Cantonal courts have to comply with federal laws regarding the storage and preservation of data and files. Therefore, article 103 of the Swiss Criminal Procedure Code also applies to cantonal (criminal) courts (see above). But there are no further provisions on the federal level providing a duty for the storage and preservation of documents (including electronic evidence) that apply to cantonal courts. Furthermore the Federal Act on Data Protection is not applicable to cantonal courts (Article 2 para

	1 e contrario). Several cantonal laws exist which rule the preservation of case documents in court trials. For example there is the Regulation of the Canton of Aargau created by the supreme body of justice, which regulates the period of preservation (there are different periods depending on the matter of the trial; § 22 of the Regulation) as well as the security standards (§ 5). The Cantonal Act on Data Protection does not apply to cantonal courts (§ 2 para 2 Act on Data Protection of the Canton of Aargau). In Berne there is a provision that determines that electronic documents will be treated as paper documents (article 7 para 1 Archiving Act of the Canton of Berne). According to Article 12, the Court of Appeal (criminal and civil proceedings) and the Administrative Court are responsible for regulating the storage and preservation of data and files. Therefore there are two Regulations; one concerning the preservation of data by civil and criminal courts; another concerning the preservation of data by administrative courts. The Regulation for civil and criminal courts regulates the period of preservation (there are different periods depending on the matter of the trial; articles 11-13) as well as the security standards (article 7 para 1). The Regulation for administrative courts is similar to the Federal Regulation. Just some trial records will be retained, the others will principally be returned to the editor (article 4). Moreover the Act on Data Protection of the Canton of Berne applies to courts as well as to other authorities (article 4 para 1 of the Act on Data Protection of the Canton of Berne). The courts are responsible for the protection and the security of the data (article 8 para 1 and article 17).
Turkey	Evidence provided during legal proceedings is conserved in the court archives according to the relevant legislation.
Ukraine	By the Law of Ukraine No. 2453-VI, of 7 July 2010, on Judiciary and Status of Judges, the Code of Commercial Procedure of Ukraine was supplemented with article 2, ‘The automated system of document flow of court’, which introduced a distribution of cases between judges on the basis of random sampling, provides for the digital archive of cases, the registration of incoming and outgoing correspondence of the court using computers, and the centralized conservation of texts of court decisions in electronic form.
UK (England & Wales)	**Lawyers** There is a duty to preserve evidence for as long as the court proceedings are live and any chance of appeal has passed. **The courts** There is a duty to preserve the court papers for the current year plus between 7 and 12 years – it will depend on the jurisdiction. However exhibits are generally returned prior to that time or held depending on the nature of the evidence and the scope for further action.

Concluding observations

73. The Terms of Reference requested:

1. An analysis of existing national legal provisions that have been adopted or adapted on the effect of electronic evidence on the rules of evidence and modes of proof, with a focus on proceedings relating to civil law, administrative law and commercial law.

2. To identify the problems that the different legal systems in the member states are faced with in this field and in respect of which they are in need of remedies or in respect of which they have put in place solutions.

3. To draw up proposals for solutions on the basis of approaches and best practice already adopted in member and other states with the objective of solving or at least reducing the workload of courts in dealing with electronic evidence in civil and administrative law proceedings.

74. From the responses received, it appears that, in the context of civil law, administrative law and commercial law, a number of existing national legal provisions have largely been adapted to reflect the reality of electronic evidence on the rules of evidence and modes of proof.

Part A

75. In part A, the types of evidence that might need to be obtained in legal proceedings were considered, and questions were asked regarding how electronic evidence might be collected or seized, taking into account the need for authenticity, what rights parties had to obtain evidence before a legal action has been initiated, and whether there are any special rules regarding the submission of evidence, especially regarding electronic signatures when submitting evidence in administrative proceedings.

76. The purpose of question 1 was to establish whether, when submitting evidence from publicly available Internet websites, it is necessary to collect the data in a specific manner to ensure the authenticity such as the use of a process server or a court appointed digital evidence specialist. Although five member states (Andorra, Croatia, France, Lithuania and Turkey) indicated ‘yes’ to the question, the more detailed responses by these member states showed that collecting the data in a specific manner was only necessary in certain circumstances, mainly where the authenticity might be in doubt. The remaining member states responding to the questionnaire revealed that there were no requirements to collect electronic evidence in a specific manner. It is concluded that the method of collection of evidence from the Internet is generally free from any specific technical requirements, and that the trier of fact assesses the authenticity and therefore weight of the evidence in accordance with the totality of the evidence.

77. In asking question 2, the aim was to establish whether it was possible to obtain electronic evidence before a legal action has been initiated on the merits. With the exception of three member states (Andorra, Armenia and Serbia), it is generally possible for a party obtain a copy of electronic data in such circumstances, although different rules might apply depending on whether (i) a party is likely to be a party to the action; (ii) where the party is not likely to be a party to the action, and (iii) where a person who is mixed up in wrongdoing. In most instances, the relevant civil procedure rules will be relevant. The type of evidence is irrelevant when a party has good reasons for obtaining evidence before legal action is initiated on the merits. This is particularly so in respect of electronic evidence, because relevant evidence is more likely to be in electronic format than any other form of evidence.

78. Given the need for a party to request electronic evidence before a legal action has been initiated on the merits, it was considered necessary to ask question 3, whether a party that is not resident in the jurisdiction to apply for the same court order as mentioned in question 2. This is important, because evidence in electronic format can reside on servers anywhere on the planet. With the exception of Andorra and Serbia, it is possible for a party in other member states that is not resident in the jurisdiction to apply for the same court order as mentioned in question 2 above.

79. Question 4 is a variation on question 1, again referring, in the main, whether, when seizing electronic evidence pursuant to a court order, the party seeking the evidence is obliged to follow a particular set of legal provisions or guidelines. Such guidelines exist for criminal proceedings, and the guidelines for criminal proceedings do not specifically apply to civil proceedings where such guidelines exist. However, the practice in some jurisdictions is for lawyers in civil proceedings to suggest to their client that obtaining electronic evidence within the guidelines for criminal proceedings helps to establish that the correct procedures were used to seize and store the evidence in such a way as not to affect its integrity and authenticity of the data.

80. The overwhelming response was that there are no guidelines that apply to the seizure of electronic evidence in civil proceedings. The conclusion must be that the lack of any guidelines for civil proceedings reflects the difference in standard of proof between criminal and civil proceedings. However, it is suggested that, because of the increase in deliberate destruction and falsification of electronic evidence, it is wise for lawyers in civil proceedings to consider following a set of guidelines where the electronic evidence is complex, such as in banking cases.

81. The report includes administrative proceedings, and question 5 sought to elicit whether there are any special rules regarding the submission of evidence in administrative proceedings, especially regarding electronic signatures. Of the responses that answered this question, 15 member states indicated there were no specific requirements. A number of member states (Croatia, Estonia, Greece, Latvia and Serbia) required an advanced electronic signature as defined under the EU Directive, and in Germany, electronic documents must be signed with a qualified electronic signature where written form is required by law. Given that administrative proceedings are largely internal to a jurisdiction and do not affect significant numbers of foreign applicants, it is not considered that this particular finding merits further consideration.

Part B

82. In part B, consideration was given to the obtaining of help from a court to establish the identity of a person, where a party claims, for instance, that an e-mail message caused damage (defamation, trade secrets, etc.) but the identity of the sender cannot be ascertained.

83. The aim in asking question 6, whether it is possible for a party to apply to a court to identify the user of an electronic service provided by a company within the jurisdiction, such as the user of an e-mail account, Internet access service, or VoIP account, was to ascertain how easy or difficult it is for a party to obtain important information that is not necessarily readily available. All of those member states responding, with the exception of Croatia, Finland, Georgia, Serbia, Slovak Republic and Ukraine, indicated that a party could apply to a court to identify the user of an electronic service provided by a company within their own jurisdiction.

84. Question 7 is an extension to question 6, asked for the purpose of ascertaining whether a party that is not resident in the country could apply for the same court order. All those responding with the exception of Belgium, Croatia, Finland, Georgia, Russian Federation, Serbia, Slovak Republic and Ukraine indicated that a party that is not resident in the jurisdiction can apply to a court to identify the user of an electronic service provided by a company within the jurisdiction, and it is possible to initiate legal action on the merits.

85. The failure of some member states to enable either their own citizens or citizens of other countries to obtain relevant information about a potential party to civil proceedings is of some concern. Given the ease by which a perpetrator can hide behind a façade of anonymity, or where they use facilities in a jurisdiction that does not enable a potential wrong party to initiate legal proceedings, it might be considered to be somewhat unfair to prevent a wronged party from obtaining relevant information with a view to considering whether they will take legal action or not.

Part C

86. In part C, covering substantive issues relating to electronic evidence, the aim was to establish how a member state had classified electronic evidence (if they did), and whether there was a presumption of reliability.

87. Question 8 enabled member states to indicate how electronic evidence had been categorised, if it was categorised. For the detailed explanation for each jurisdiction, please see the individual response and the outline provided in the table to this question, but generally evidence is presumed reliable unless challenged by the opposing party. Taking the matter one stage further, question 9, sought to establish whether there is a presumption relating to electronic evidence being “reliable”, “in order”, “accurate”, “properly set or calibrated” or “working properly”. The only jurisdiction in which there is an explicit presumption regarding computers being reliable is that of England & Wales, and it is the topic of criticism.[20] In civil proceedings in England & Wales, there is a presumption of authenticity of all forms of evidence, and it is for the opposing party to raise the question of authenticity under the Civil Procedure Rules (CPR 32.19). The position is similar in Estonia, in that that all evidence is presumed reliable unless the opposing party challenges the evidence, then the evidence must be authenticated. The position is not certain in Montenegro. In the Russian Federation, there is a presumption where electronic data are obtained in the manner prescribed by law. In Spain a presumption will apply, depending on whether data in digital format is ‘signed’ by an advanced electronic signature. There is no such presumption in the other jurisdictions submitting responses to the questionnaire.

88. From a practical point of view, taking into account the lower standard of proof in civil proceedings, a presumption of the authenticity of all forms of evidence is a helpful presumption that relieves parties of the need to prove every item of evidence – especially when both parties might not challenge the evidence. Where a party does challenge the evidence, then the party seeking to submit the evidence will need to demonstrate authenticity. Additionally, where certain procedures are used, such as advanced electronic signatures, or where independent and officially recognised external agencies such as bailiffs obtain evidence independently of the parties, the need for strict rules relating to the authenticity of the evidence need not be tested – unless, that is, one party disputes the evidence. However, the presumption in England & Wales that computers are reliable is a dangerous one, and a presumption that is not demonstrated by any evidence.

[20] For a detailed critique, see Stephen Mason, gen ed, *Electronic Evidence* (3rd ed, LexisNexis Butterworths, 2012), chapter 5.

Part D

89. In part D, regarding the admissibility of electronic evidence, the purposes was to establish whether it was necessary to use a specific procedure to obtain electronic evidence (as is the case in criminal proceedings), and if not, whether the court would consider how the evidence was obtained in deciding whether to admit the evidence. This was the topic of question 10. The replies indicate that no member state has a legal requirement to obtain electronic evidence using a specific procedure, although civil procedure rules might apply regarding the obtaining and admission of evidence. Question 11 covered the position where, if electronic evidence were not obtained in accordance with any standard or special procedure, whether the court would take this into account in deciding whether to admit the evidence. In general, the response was that a court would evaluate the evidence before it in the normal course of judicial proceedings, taking into account all of the technical evidence made available. In some jurisdictions, the judge will decide what evidence to accept and what evidence to have tested for authenticity.

90. A variation on this theme was followed in question 12, where it was asked whether any technical guidelines or best practices have been published that describe how electronic evidence can be obtained while maintaining its integrity. Guidelines have not been produced by member states other than in Poland – and these might not cover civil proceedings – and in England & Wales in respect of criminal cases, but not civil proceedings. In Germany, there is a limited presumption regarding integrity where an individual has registered securely for a 'De-Mail' account, and in Montenegro, the Law on Electronic Signature provides for the creation of a set of rules relating to advanced electronic signatures, which, if followed, provide for a presumption of reliability.

91. In framing question 13, the issue was whether the rules on the admissibility of electronic evidence varied according to the complexity or simplicity of the evidence. The overwhelming response was that the rules on the admissibility of electronic evidence tend not to vary. The amount of evidence to demonstrate the authenticity of digital data may alter, depending on the complexity of the evidence.

Part E

92. In part E, the intention was to establish what, if any, rules were in place relating to the duty and requirements for the storage and preservation of electronic evidence for lawyers and the courts, and the requirements to provide for the security of evidence after a trial.

93. The position regarding the archiving and security of electronic data by lawyers and the courts appears to be somewhat confusing. Where a member state is also a member of the EU, the relevant Directive on data protection applies[21] – in particular, the provisions of article 17 'Security of processing'. The CCBE guidelines and national professional guidelines (where they exist) might also cover this point. A number of responses from member states indicate that the duties of courts and lawyers regarding the security client data are not well understood. The position under the legislation is clear in the European Union, and to illustrate the importance of this issue, on 2 November 2015, the Crown Prosecution Service in England & Wales was the subject of a Monetary Penalty Notice of £200,000 from the Office of the Information Commissioner after laptops containing videos of police interviews were stolen from a private film studio. The interviews were with 43 victims and witnesses.

[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31 – 50.

They involved 31 investigations, nearly all of which were ongoing and of a violent or sexual nature.[22]

94. Member states need to consider this aspect of electronic evidence robustly, and from a number of points of view, including: safe keeping; effective deletion (that is, expunging data), and exceptions regarding historical cases. Lawyers have a professional duty towards their clients, and the fact that their correspondence is a mix of paper and electronic communications does not absolve them of their duty to provide for the proper security of electronic documents.

[22] https://ico.org.uk/media/action-weve-taken/mpns/1560074/crown-prosecution-service-monetary-penalty-notice.pdf.

Existing Committee of Ministers recommendations

95. The CDCJ was also requested to assess the following Committee of Ministers recommendations, and whether they require revision, and if so, to make appropriate proposals:

> Recommendation No. R (86) 12 concerning measures to prevent and reduce the excessive workload in the courts
>
> Recommendation No. R (95) 11 on the selection, processing, presentation and archiving of court decisions in legal information retrieval systems
>
> Recommendation Rec(2001)2 concerning the design and re-design of court systems and legal information systems in a cost-effective manner
>
> Recommendation Rec(2001)3 on the delivery of court and other legal services to the citizen through the use of new technologies
>
> Recommendation Rec(2003)14 on the interoperability of information systems in the justice sector
>
> Recommendation Rec(2003)15 on archiving of electronic documents in the legal sector

96. It is not considered necessary to re-visit Recommendation No. R (86) 12, dealing, as it does, with the workload of courts.

97. It is suggested that courts might be usefully reminded of the provisions of Recommendation No. R (95) 11, now that greater use is made of placing judgments online, together with Recommendation Rec(2003)15.

98. It will be of interest to revise Recommendation Rec(2001)2, Recommendation Rec(2001)3 and Recommendation Rec(2003)14, taking into account the variety of work being undertaken – especially in the European Union – that partially reflects of the provisions of these Recommendations.

Appendix A

Terms of Reference

for a comparative study on the effect of electronic evidence on the rules of evidence and modes of proof

The consultants shall:

1. Undertake a comparative study and analysis of existing national legal provisions that have been adopted or adapted on the effect of electronic evidence (which, by its very nature, includes the Internet and new technologies) on the rules of evidence and modes of proof, with a focus on proceedings relating to civil law, administrative law and commercial law.

2. Identify the problems that the different legal systems in the member states are faced with in this field and in respect of which they are in need of remedies or in respect of which they have put in place solutions.

3. Draw up proposals for solutions on the basis of approaches and best practice already adopted in member and other states with the objective of solving or at least reducing the workload of courts in dealing with electronic evidence in civil and administrative law proceedings.

The study should deal with, but not exclusively, issues relating to the admissibility of electronic evidence, the weight given to electronic evidence, the implications for credential rules such as burden of proof and presumptions, authenticity/reliability, archiving and preservation of evidence, case and trial management, the role of the judge, pre-trial search for evidence, the role of independent or court experts.

The comparative study shall take into account information supplied by members of the European Committee on Legal Co-operation (CDCJ) on the basis of a questionnaire to be prepared by the consultants or on reply to a preliminary draft prepared by the consultants.

In the light of the above-mentioned analysis, the consultants shall also consider to what extent the Committee of Ministers recommendations[23] relevant to the use of information and communication technologies by courts require revision, and make proposals.

[23] Recommendation No. R (86) 12 concerning measures to prevent and reduce the excessive workload in the courts;

Recommendation No. R (95) 11 on the selection, processing, presentation and archiving of court decisions in legal information retrieval systems;

Recommendation Rec(2001)2 concerning the design and re-design of court systems and legal information systems in a cost-effective manner;

Recommendation Rec(2001)3 on the delivery of court and other legal services to the citizen through the use of new technologies;

Recommendation Rec(2003)14 on the interoperability of information systems in the justice sector;

Recommendation Rec(2003)15 on archiving of electronic documents in the legal sector.

Appendix B

Questionnaire

on the use of electronic evidence

in civil and administrative law proceedings

and its impact on the rules of evidence and modes of proof

A. Obtaining electronic evidence

Preamble

There are three types of evidence that might need to be obtained in legal proceedings:

(i) Evidence from publicly available websites, such as (this list is only indicative) blog postings and images uploaded to social networking websites.

(ii) The substantive evidence (or evidence of content), that is the e-mail or documents in digital format that are not made publicly available and which are held on a server.

(iii) Purported user identity and traffic data ('meta data') that is used to help identify a person by finding out the source of the communication, but not the content.

For instance, a jurisdiction problem arises if a French company believes an employee has stolen trade secrets and stored the data on a British private cloud service.

Questions

1. If a party wants to submit evidence from publicly available internet websites, will a court customarily require that the copies of websites be collected in a specific manner to ensure the authenticity, such as the use of a process server or a court appointed digital evidence specialist?

   Yes ☐
   No ☐

   If the answer is 'yes' please provide further details, including any relevant legal principles.

2. Is it possible for a party to apply to a court to obtain a copy of electronic data (such as computer files stored on a computer of a third party within the jurisdiction) before a legal action has been initiated on the merits?

   Yes ☐
   No ☐

   If the answer is 'yes' please provide further details, including any relevant legal principles.

3. Is it possible for a party that is not resident in your country to apply for the same court order as mentioned in 2 above, and is it also possible even if it is unlikely that the legal action on the merits will be litigated before a national court?

   Yes ☐
   No ☐

   If the answer is 'yes' please provide further details, including any relevant legal principles:

4. When seizing electronic evidence pursuant to a court order, is the party seeking the evidence obliged to follow any particular set of legal provisions or guidelines for seizing electronic evidence

   Yes ☐
   No ☐

   If the answer is 'yes' please provide further details, including any relevant legal principles:

5. Regarding administrative proceedings, please indicate whether there are any special rules regarding the submission of evidence, especially regarding electronic signatures, and whether a specific form of electronic signature is required when submitting evidence electronically.

B. Obtaining purported user identification

Preamble

The problem arises when a party claims that an e-mail message caused damage (defamation, trade secrets, etc.) but the identity of the sender cannot be ascertained. The party that has suffered a wrong uses the identifying information from the e-mail provider (meta-data) to prove the connection between an e-mail account and a natural person, that is, the e-mail user.

Questions

6. Is it possible for a party to apply to a court to identify the user of an electronic service provided by a company within your jurisdiction, such as the user of an e-mail account, internet access service, or VoIP account[24]?

   Yes ☐
   No ☐

   If the answer is 'yes' please provide further details, including any relevant legal principles:

[24] VOIP (voice-over internet protocol): a system for converting analogue signals to digital so that telephone calls may be made over the internet.

7. Is it possible for a party that is not resident in your country to apply for the same court order, and is it also possible if it is unlikely that the legal action on the merits will be litigated before a national court?

   Yes ☐
   No ☐

   If the answer is 'yes' please provide further details, including any relevant legal principles:

C. Substantive issues regarding the nature of electronic evidence.

Preamble

To a certain extent, electronic evidence is a still relatively new concept. Our aim in asking questions in this section is to assess how different jurisdictions are dealing with electronic evidence in legal proceedings. Article 9 of the EU Directive 2000/31 on E-Commerce requires Member States to allow for electronic contracting in a manner that it does not create obstacles for their validity; see also article 4-2 of the EU Directive 1999/93 on Electronic Signatures.

Questions

8. Please set out the classifications of evidence, if any, and how electronic evidence fits into the classification. For example, are certain types of electronic evidence presumed authentic and reliable and are there other types that are presumed unreliable?

9. Is there a presumption in your jurisdiction relating to electronic evidence regarding it being "reliable", "in order", "accurate", "properly set or calibrated" or "working properly"?

   Yes ☐
   No ☐

   If the answer is 'yes' please provide further details, including any relevant legal principles.

D. The admissibility and integrity of electronic evidence

Preamble

Many jurisdictions have provided for the admissibility of electronic evidence into legal proceedings. This issue has also been addressed regionally, such as the provision of article 5(2) of the European Union Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,[25] which provides that an electronic signature cannot be 'denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form'. Similarly the provision of article 9(1) of the European Union Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'),[26] provides that contracts shall not be deprived of legal effectiveness and validity

[25] OJ L 13, 19.1.2000, p.12. The Directive will be repealed by Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, pp. 73 – 114.
[26] OJ L 178, 17.7.2000, pp. 0001 – 0016.

on account of their having been made by electronic means. It is generally accepted that evidence in electronic format is admissible in legal proceedings. Rules might include:

(i) whether the evidence should be obtained in accordance with any technical guidance, (for instance, guidelines exist for criminal proceedings, and they can be useful for civil and administrative proceedings[27]), and

(ii) how the authenticity and reliability of electronic evidence is determined – that is, whether there are any agreed guidelines laid down that helps a judge determine the authenticity of electronic evidence, and if there is any presumption regarding the 'reliability' of electronic evidence.

Questions

10. Is a party wishing to submit electronic evidence in civil or administrative proceedings, required to have obtained it using a specific procedure, as required by law or otherwise?

    Yes ☐
    No ☐

    If the answer is 'yes' please provide further details, including any relevant legal principles.

11. If electronic evidence is not obtained in accordance with any standard or special procedure, will the court take this into account in deciding whether to admit the evidence?

    Yes ☐
    No ☐

    If the answer is 'yes' please provide further details, including any relevant legal principles.

12. If not already mentioned elsewhere in your response, are there any technical guidelines or best practices that have been published in your country that describe how electronic evidence can be obtained while maintaining its integrity?

    Yes ☐
    No ☐

    If the answer is 'yes' please provide further details, including any relevant legal principles.

[27] For example: *Guidelines for Best Practice in the Forensic Examination of Digital Technology*, Version 6 (20 April 2009), European Network of Forensic Science Institutes, Forensic Information Technology Working Group, available at http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf; UK Association of Chief Police Officers 'Good Practice Guide for Digital Evidence', Version 5 (October 2011), available at http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf

13. Do the rules on admissibility of electronic evidence vary according to the complexity or simplicity of the evidence?

    Yes ☐
    No ☐

    If the answer is 'yes' please provide further details, including any relevant legal principles.

E. The archiving of evidence after trial

Preamble

Electronic evidence needs to be treated differently than paper files and case exhibits. By printing electronic documents, the relevant metadata that goes to prove the authenticity of the document is lost. This means that is it necessary to retain electronic data in its original form for as long as a paper case file would be retained. To this extent, it is necessary for lawyers and court administrators to provide for the confidentiality and security of such data, including the retention of secure back-up copies should one of the means of storage fail.

The Council of Bars and Law Societies of Europe (CCBE) have produced a set of guidelines dealing specifically with 'cloud computing', which is tangential to this study, but there is no other guidance provided by the CCBE that directly covers this topic.[28]

Question

14. What are the norms or professional conduct, if any, relating to the duty and requirements for the storage and preservation of electronic evidence?

    In reply to this question, please cover the following discrete areas:

    - Archiving by lawyers
    - Archiving by the courts
    - Requirements to provide for the security of evidence after a trial.

[28] *CCBE guidelines on the use of cloud computing services by lawyers*, available at http://www.ccbe.eu/.