Competence Center
Steuern und Recht

«VOI»

»Legal Requirements for Document Management in Europe«

Coordination:	**Jürgen Biffar** (DocuWare)
	Stefan Groß (Peters, Schönberger & Partner)
Austria:	**Markus Andréewitch** (Andreéwitch & Simon), **Herbert F. Maier**
France:	**Philippe Martin** (Bureau von Dijk) **et. al.**
Germany:	**Stefan Groß** (Peters, Schönberger & Partner)
Italy:	**Andrea Lisi** (Studio Legale Lisi)
Spain:	**Alberto Olivares Antolín** (Ernst & Young)
Switzerland:	**Marc Philipp Gugger** (Ernst & Young)
United Kingdom:	**Alan Shipman** (Group 5 Training)

VOI – Verband Organisations- und Informationssysteme e.V.
Heilsbachstr. 25, 53123 Bonn, Germany
www.voi.de

SPONSORS:

DocuWare

EASY SOFTWARE

Scope

The competence center for "Steuern und Recht" (tax and law) of the German trade association for document management industry (**Verband Organisations- und Informationssysteme e.V. - voice of information – VOI**) has initiated this publication setting out the main legal aspects for document management in European countries.

The publication is designed to offer simple and short descriptions of the legal requirements which have to be observed in major European countries when documents are stored electronically for long term archiving purposes. It aims to provide support and offer valuable information to software vendors, consultants and end users acting on a Europe-wide basis.

May 2011

Disclaimer

The information provided in this publication is without engagement and is intended solely to provide you with a general overview of the problems without any pretension to completeness or accuracy of detail. This publication is not designed to clarify the details of individual legal regulations or all aspects of the subjects addressed and does not replace legal and tax advice in individual cases. Before making any business decisions you should consult your tax adviser, auditor or attorney. The legal regulations may have changed since this text was published.

Table of Contents

Austria

Authors:

Dkfm. Herbert F. Maier
Wirtschaftsprüfer und Steuerberater/certified accountant and tax advisor

1010 Wien, Walfischgasse 5-7

www.hfmaier.at

office@hfmaier.at

Dr. Markus Andréewitch
Rechtsanwalt/attorney-at-law

1010 Wien, Stallburggasse 4

www.andsim.at

office@andsim.at

1. Unternehmensrechtliche Aspekte

1.1. Rechtsgrundlagen

§ 212 UGB regelt die unternehmensrechtliche Aufbewahrungspflicht und Aufbewahrungsfrist; nach § 190 Abs 5 UGB kann der Unternehmer zur ordnungsgemäßen Buchführung und zur Aufbewahrung seiner Geschäftsbriefe Datenträger benützen; die Vorlage von Unterlagen auf Datenträgern ist in § 216 UGB geregelt.

1.2. Aufbewahrungspflichtige

Der Aufbewahrungspflicht unterliegen nach § 212 Abs 1 UGB Unternehmer, d. s.:

- Kapitalgesellschaften und unternehmerisch tätige Personengesellschaften, bei denen kein unbeschränkt haftender Gesellschafter eine natürliche Person ist;
- alle anderen Unternehmen mit einem Umsatz von mehr als EUR 400.000,00. Die Rechnungslegungspflicht ist unabhängig von der Eintragung in das Firmenbuch.

Ausgenommen von der Rechnungslegungspflicht sind gemäß § 189 Abs 4 UGB Angehörige der freien Berufe, Land- und Forstwirte sowie Unternehmer, deren Einkünfte iSd EStG aus dem Überschuss der Einnahmen über die Werbungskosten bestehen.

1. Corporate law aspects

1.1. Legal foundations

§ 212 of the Unternehmensgesetzbuch (UGB – Commercial Code) specifies safekeeping obligations and safekeeping periods for enterprises; according to § 190 Sec. 5 of the UGB, an enterprise may use data carriers for orderly bookkeeping and documentation of business correspondence; presentation of documents on data carriers is governed by § 216 of the UGB.

1.2. Parties responsible for safekeeping

According to § 212 Sec. 1 of the UGB, enterprises obliged to safekeeping include:

- Corporations and entrepreneurial partnerships none of whose partners with unlimited liability is a natural person.
- All other companies with a turnover of more than EUR 400,000.00. Accounting obligations apply irrespective of the entry in the commercial register.

Exempt from accounting obligations according to § 189 Sec. 4 of the UGB are the liberal professions, agriculture and forestry, as well as enterprises whose earnings in the sense of income tax laws consist of revenues in excess of professional expenses.

1.3. Aufbewahrungsumfang

Nach § 212 UGB hat der Unternehmer folgende Unterlagen aufzubewahren:

- Inventare
- Eröffnungsbilanzen
- Jahresabschlüsse samt den Lageberichten
- Konzernabschlüsse samt den Konzernlageberichten
- empfangene Geschäftsbriefe
- Abschriften der abgesendeten Geschäftsbriefe und
- Belege für Buchungen in den von ihm gemäß UGB zu führenden Büchern (Buchungsbelege)

1.3. Scope of safekeeping

According to § 212 of the UGB, entrepreneurs must consign the following documents to safekeeping:

- Inventories
- Opening balance sheets
- Annual financial statements and reports
- Consolidated financial statements and reports
- Business letters received
- Copies of business letters sent
- Records (accounting receipts) for postings made in the books to be kept by the entrepreneur as per the UGB

1.4. Umfang der Vorlagepflicht von Unterlagen auf Datenträgern

Wer Eintragungen oder Aufbewahrungen in elektronischer Form vorgenommen hat, muss, soweit er zur Einsichtgewährung verpflichtet ist, gemäß § 216 UGB auf seine Kosten innerhalb angemessener Frist diejenigen Hilfsmittel zur Verfügung stellen, die notwendig sind, um die Unterlagen lesbar zu machen, und, soweit erforderlich, die benötigte Anzahl ohne Hilfsmittel lesbarer, dauernder Wiedergaben beibringen.

1.4. Scope of obligations as concerns submission of records on data carriers

To the extent an entrepreneur is committed to disclosing electronic entries and records according to § 216 of the UGB, the entrepreneur must, at his/her own expense and within a reasonably short period of time, provide the aids necessary for reading the records as well as the required, lasting reproductions which can be read without aids

1.5. Aufbewahrungsart

§ 212 UGB bestimmt, dass eine gesonderte Aufbewahrung geordnet zu erfolgen hat.

Der Unternehmer kann zur ordnungsgemäßen Buchführung und zur Aufbewahrung seiner Unterlagen Datenträger benützen.

1.5. Safekeeping technique

According to § 212 of the UGB, safekeeping must be discrete and organized.

The entrepreneur may use data carriers for orderly bookkeeping and maintenance of records.

Hierbei muss die inhaltsgleiche, vollständige und geordnete, hinsichtlich der in § 212 Abs 1 UGB genannten Schriftstücke auch die urschriftgetreue Wiedergabe der gespeicherten Daten bis zum Ablauf der gesetzlichen Aufbewahrungsfristen jederzeit gewährleistet sein.

In this connection, it is necessary to ensure that the stored data can at all times be reproduced consistently in terms of content, fully, in an organized manner and - as concerns documents mentioned in § 212 Sec. 1 of the UGB - true to the original documents until expiry of the statutory safekeeping deadlines.

1.6. Aufbewahrungsort

Ein bestimmter Ort der Aufbewahrung ist nicht vorgeschrieben. Die Unterlagen müssen jedenfalls innerhalb angemessener Zeit vorgelegt werden können. Unter dieser Voraussetzung kann der Aufbewahrungsort nach Unternehmensrecht auch im Ausland liegen.

1.6. Safekeeping sites

Safekeeping sites have not been prescribed. At any rate, it must be possible to present documents within a reasonably short period of time. Provided that this condition is fulfilled, commercial law also permits safekeeping sites to be located abroad.

1.7. Aufbewahrungsfrist

Grundsätzlich beträgt die Aufbewahrungsfrist nach UGB sieben Jahre. Eine Verlängerung der Aufbewahrungsfrist tritt für die Dauer eines anhängigen gerichtlichen oder behördlichen Verfahrens ein, in dem der Unternehmer Parteistellung hat.

1.7. Safekeeping periods

The UGB prescribes a basic safekeeping period of seven years. The safekeeping period is extended by the duration of any pending judicial or official proceedings in which the entrepreneur is a party.

1.8. Sanktionen

Das UGB sieht einen direkten Zwang zur Erfüllung der öffentlich-rechtlichen Buchführungspflicht grundsätzlich nicht vor. Indirekter Zwang geht von der Prüfungspflicht des Firmenbuchgerichtes und der Zwangsstrafendrohung, von den gesellschaftsrechtlichen Rechnungs-legungsvorschriften und Haftungs-tatbeständen, ferner von Bestimmungen des Insolvenzrechts und anderen Strafdrohungen des Strafgesetzbuches sowie von steuerrechtlichen Vorschriften aus.

1.8. Sanctions

In principle, the UGB does not impose a direct compulsion mechanism to fulfill accounting requirements prescribed under public law. An indirect compulsion mechanism is imposed by commercial register court audit requirements, threat of penalty payments, corporate accounting regulations, liability issues, bankruptcy laws, penalties under the penal code, and tax laws.

2. Steuerrechtliche Aspekte

2.1. Rechtsgrundlagen

Für den Bereich des Steuerrechts sind die Bestimmungen der BAO maßgeblich. Nach § 132 Abs 2 BAO kann die Aufbewahrung dieser Unterlagen auf Datenträgern unter bestimmten Voraussetzungen erfolgen.

2.2. Aufbewahrungspflichtige

Die Aufbewahrungspflicht nach § 132 BAO trifft alle Personen (Unternehmer, Abgabenpflichtige), die Buchführungspflichten zu erfüllen haben. Diese Pflicht trifft aber nicht nur die zur Buchführung Verpflichteten, sondern auch die freiwillig Bücher führenden Personen. Der Kreis der Aufbewahrungspflichtigen nach BAO ist größer als der Kreis der Aufbewahrungspflichtigen nach UGB.

2.3. Umfang der Aufbewahrungspflichten

Die gesamten Daten der Buchführung unterliegen der Aufbewahrungspflicht. Mit der Erfüllung der abgabenrechtlichen Aufbewahrungspflichten sind die unternehmensrechtlichen Aufbewahrungspflichten jedenfalls abgedeckt.

2.4. Umfang der Vorlagepflicht von Unterlagen auf Datenträgern

§ 132 Abs 3 BAO bestimmt den Umfang der Vorlagepflicht von auf Datenträgern aufbewahrten Belegen, Geschäftspapieren und sonstigen Unterlagen analog zu § 216 UGB (vgl. dazu Pkt. 1.4.).

2. Tax law aspects

2.1. Legal foundations

The Federal Taxation Code is authoritative in terms of tax laws. According to § 132 Sec. 2 of the Bundesabgabenordnung (BAO - Federal Taxation Code), related documents can be stored on data carriers under certain conditions.

2.2. Parties responsible for safekeeping

According to § 132 of the BAO, responsibility for safekeeping applies to all persons (entrepreneurs, persons liable to pay tax) obliged to comply with accounting obligations. Apart from the persons obliged to comply with accounting obligations, this responsibility also applies to persons who voluntarily maintain accounts. Compared with the UGB, the BAO defines a larger group of parties responsible for safekeeping.

2.3. Scope of safekeeping commitments

All accounting data are subject to a safekeeping commitment. Fulfillment of the safekeeping obligation prescribed by tax law at any rate ensures fulfillment of the safekeeping obligation prescribed by corporate law.

2.4. Scope of obligations as concerns submission of records on data carriers

§ 132 Sec. 2 BAO describes the scope of obligations as concerns submission of receipts, business papers and other documents on data carriers, § 216 UGB is applied mutatis mutandis (see section 1.4).

2.5. Aufbewahrungsart

Erfolgt die Aufbewahrung von aufbewahrungspflichtigen Unterlagen auf Datenträgern, muss die vollständige, geordnete, inhaltsgleiche und urschriftgetreue Wiedergabe bis zum Ablauf der gesetzlichen Aufbewahrungsfrist jederzeit gewährleistet sein.

2.5. Safekeeping technique

If documents subject to safekeeping are stored on data carriers, it should be possible to reproduce their content completely, in a systematic manner, accurately and true to the original at all times right up to expiry of the statutory safekeeping deadline.

2.6. Ort der Aufbewahrung

§ 131 Abs 1 BAO bestimmt unter anderem, dass Bücher und Aufzeichnungen auf Verlangen der Abgabenbehörde innerhalb angemessen festzusetzender Frist in das Inland zu bringen sind.

Die Erlaubnis, Grundaufzeichnungen im Ausland zu führen und dort aufzubewahren, sowie die Pflicht, diese Unterlagen auf Verlangen innerhalb angemessener Frist ins Inland zu bringen, gilt hinsichtlich jener Vorgänge, die einem im Ausland gelegenen Betrieb, einer im Ausland gelegenen Betriebsstätte oder einem im Ausland gelegenen Grundbesitz zuzuordnen sind.

Die übrigen Grundaufzeichnungen dürfen zwar im Ausland geführt werden, sind aber innerhalb angemessener Frist ins Inland zu bringen und dort aufzubewahren. Es dürfte ausreichen, wenn der Produktivserver (für den Tagesbetrieb) im Ausland steht, aber im Inland Backup Kopien etc. vorgenommen werden, dies ist aber derzeit nicht endgültig geklärt.

2.6. Safekeeping site

According to § 131 1 Sec. of the BAO, books and records should be transferable inland within an appropriate deadline on request by tax authorities.

The permission to maintain and store basic records abroad and the obligation to transfer these records to Austria within an appropriate deadline on request apply to processes associated with businesses, premises and properties located abroad.

Though the remaining basic records may be maintained abroad, it must be possible to transfer them to Austria within a reasonable period of time and maintain them there. It should be sufficient if the operative server (for the day-to-day operations) is abroad as long as back-up copies are maintained in Austria; this position is not yet finally determined.

2.7. Aufbewahrungsfrist

Die Aufbewahrungsfrist beträgt gemäß § 132 Abs 1 BAO grundsätzlich sieben Jahre. Die Frist für die Aufbewahrung von Aufzeichnungen und Unterlagen, die Grundstücke betreffen, verlängert sich auf 12 Jahre, für bestimmte Grundstücke sogar 23 Jahre (§18 Abs 10 UStG). Zudem sind auch in einem anhängigen Abgaben oder Gerichtsverfahren die Unterlagen trotz Fristenablaufs weiter aufzubewahren.

2.7. Safekeeping periods

§ 132 Sec. 1 of the BAO prescribes a basic safekeeping period of seven years. Records and documents concerning properties are subject to an extended safekeeping period of 12 years and 23 years for certain properties (§ 18 Sec. 10 Austrian Sales Tax Law (UStG). To the extent tax or court proceedings are pending, the records and documents must be retained even through such time periods have already expired.

2.8. Sanktionen

Als Finanzordnungswidrigkeit ist die (vorsätzliche) Verletzung der Bücher, Aufzeichnungen und hiezu gehörige Belege umfassenden Aufbewahrungspflicht ahndbar.

2.8. Sanctions

Intentional manipulations of books, records and associated receipts subject to safekeeping constitute breaches of financial law and are punishable.

2.9. Umsatzsteuer und elektronisch übermittelte Rechnungen

Ein Unternehmer kann unter folgenden Voraussetzungen seine Rechnungen ausschließlich elektronisch übermitteln:

- Der Rechnungsempfänger muss die elektronische Rechnung akzeptieren.
- Die Echtheit der Herkunft und die Unversehrtheit des Inhaltes einer elektronischen Rechnung müssen gewährleistet sein.

Die Vorschriften des Umsatzsteuergesetzes hinsichtlich der Rechnungsbestandteile müssen eingehalten werden. Die Echtheit der Herkunft und die Unversehrtheit des Inhaltes sind gewährleistet, wenn die Rechnung mit einer (sog. -fortgeschrittenen“) - elektronischen Signatur versehen ist - oder im Rahmen des EDI-Verfahrens übermittelt werden. Telefax- oder E-Mail-Rechnungen sind elektronisch übermittelte Rechnungen. Bis zum Ende des Jahres 2011 können Rechnungen weiterhin mittels Fernkopierer (Telefax) übermittelt werden. Für Telefax bedarf es daher bis dahin keiner fortgeschrittenen elektronischen Signatur.

Der EU-Ministerrat hat am 13.7.2010 die Änderungen der Mehrwertsteuersystem-richtlinie (2006/112/EG), die den Einsatz von elektronischen Rechnungen fördern soll, verabschiedet. Es werden danach an elektronische Rechnungen keine weitergehenden Anforderungen als an Papierrechnungen gestellt. Die elektronischen Rechnungen sind nach Zustimmung des Empfängers anzuerkennen, wenn ihre Echtheit, die Unversehrtheit des Inhalts und die Lesbarkeit gewährleistet ist.

2.9. Sales tax and electronic invoices

An entrepreneur may submit invoices exclusively in electronic format if the following conditions are fulfilled:

- The recipient accepts electronic invoices.
- The electronic invoice's authenticity and integrity of its contents must be ensured.

Sales tax regulations concerning invoice items shall be observed. Authenticity and integrity of contents are ensured if the invoice is furnished with a (so-called advanced) electronic signature or is transmitted by electronic data interchange. Invoices submitted via fax or e-mail are considered electronic invoices. Until the end of 2011, invoices may still be submitted by fax. Therefore, a fax does not require an advanced electronic signature.

On 13 July, 2010 the Council Directive (2006/112/EG) on the common system of sales tax was enacted, it is intended to enhance the use of electronic invoices. Pursuant thereto, no additional requirements may be demanded of electronic invoices as are required of paper invoices. The electronic invoices are sufficient if accepted by the recipient, provided that the authenticity of the origin and the integrity of their content and the readability are guaranteed.

Die Richtlinie enthält keine verbindlichen Vorgaben für die Archivierung. Die Mitgliedstaaten können ausdrücklich die Aufbewahrung in Originalform verlangen sowie die Archivierungsdauer selbst bestimmen. Vorgeschlagen wurde von der EU-Kommission eine einheitliche Frist von sechs Jahren. Die Mitgliedstaaten müssen die genannte Richtlinie bis 31.12.2012 in nationales Recht umsetzen.

The directive has no binding requirements for archiving. The member states may expressly require the safekeeping in original form and determine the term thereof. The commission suggests a uniform term of six years. The member states must transpose the directive by 31 December 2012 at the latest.

3. Zivilrechtliche Aspekte

3. Civil law aspects

3.1. Beweismittelkraft elektronischer Urkunden im Vergleich

3.1. Comparison of the validity of electronic documents as evidence

Der zentrale Grundsatz in österreichischen Zivil- und Strafverfahren ist jener der freien Beweiswürdigung. Danach hat das Gericht unter sorgfältiger Berücksichtigung der Ergebnisse der gesamten Verhandlung und Beweisführung nach freier Überzeugung zu beurteilen, ob eine tatsächliche Angabe für wahr zu halten sei oder nicht. In seiner Urteilsbegründung muss das Gericht aber offenlegen, aufgrund welcher Erfahrungssätze es zur Auffassung gelangt ist, die festgestellten Tatsachen seien für wahr zu halten.

A central concept of Austrian civil and criminal proceedings is that of free assessment of evidence. Accordingly, a court must at its own discretion carefully consider the results of proceedings and evidence in their entirety in order to ascertain the veracity of submitted details. When providing reasons for its judgment, the court must declare which professional experiences it has used as a basis for establishing the veracity of the circumstances under consideration.

Dieser fundamentale Grundsatz gilt im Zivilprozess für alle Beweismittel, also nicht nur für Zeugenaussagen, sondern insbesondere auch für die dem Gericht vorgelegten Urkunden, unabhängig davon, ob diese in schriftlicher oder elektronischer Form abgefasst sind (also insbesondere für E-Mail-Ausdrucke, Faxausdrucke, gescannte Urkunden, etc.).

In civil proceedings, this basic concept applies to all items of evidence, i.e. not just witnesses' statements but also, in particular, documents submitted to the court, regardless of whether they are in written or electronic form (including printouts of e-mails and facsimiles, scanned documents etc.).

Im Zivilverfahren wird zwischen öffentlichen Urkunden und Privaturkunden unterschieden. Öffentliche Urkunden sind die von einer österreichischen öffentlichen Behörde, einer mit öffentlichen Glauben versehenen Urkundsperson oder von einer ausländischen öffentlichen Behörde ausgestellten Urkunden. Alle anderen Urkunden sind Privaturkunden. Für öffentliche Urkunden gilt die Vermutung der Echtheit, dass sie also von dem in ihr angegebenen Aussteller stammen. Bei Privaturkunden gibt es diese Echtheits-vermutung nicht.

Civil proceedings differentiate between public and private documents. Public documents are documents issued by an Austrian public authority, a publicly certified notary, or a foreign public authority. All other documents are private. Public documents are assumed as being authentic, i.e. as originating from the declared source. This assumption of authenticity is not made in the case of private documents.

Ist allerdings die Privaturkunde unterfertigt, begründet dies den vollen Beweis dafür, dass die darin enthaltenen Erklärungen vom Namensträger der Unterschrift stammen. Nach österreichischem Recht gibt es daher auch nicht unterfertigte Privaturkunden (z.B. Internetausdrucke, Pläne).

If a private document has been undersigned, however, it is full proof that the statements therein originate from the person who affixed their signature. Under Austrian law therefore, also unsigned private documents exist (e.g. internet print-outs, plans).

In Übereinstimmung dazu legt das österreichische Signaturgesetz (§ 4 Abs. 3) fest, dass die Bestimmungen der Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde auch auf elektronische Dokumente anzuwenden sind, die mit einer qualifizierten elektronischen Signatur versehen sind.

In concurrence, the Austrian signature law (§ 4 Sec. 3) stipulates that the assumption of authenticity of an undersigned document's contents also applies to electronic documents furnished with a qualified, electronic signature.

Weiters begründen öffentliche Urkunden vollen Beweis dessen, was darin von der Behörde amtlich verfügt, erklärt oder bezeugt wird. Dies gilt für Privaturkunden nicht. Die inhaltliche Richtigkeit von Privaturkunden unterliegt stets der freien richterlichen Beweiswürdigung.

Furthermore, public documents fully substantiate the official decrees, statements and attestations contained therein. This does not apply to private documents. The correctness of any private document's contents is subject to assessment of evidence by a court at its own discretion.

Die dargestellten Regelungen zu dem Urkundenbeweis bezüglich öffentlicher Urkunden und Privaturkunden gelten für das Strafverfahren nicht. Dort entscheidet der Richter nicht nach gesetzlichen Beweisregeln, sondern nur nach seiner freien, aus der gewissenhaften Prüfung aller für und wider vorgebrachten Beweismittel gewonnenen Überzeugung. Im Zweifel ist dabei stets zugunsten des Angeklagten zu entscheiden (in dubio pro reo).

These rules concerning the authenticity of public and private documents do not apply in the case of criminal proceedings. In this case, the judge makes their decision not on the basis of statutory rules concerning validity of evidence, but on the basis of their own, independent conviction arising from a conscientious examination of all items of evidence, pro as well as contra. In case of doubt, judgment should always be passed in favor of the accused (in dubio pro reo).

Im Verwaltungsverfahren wird hinsichtlich des Urkundenbeweises auf die Bestimmungen der Zivilprozessordnung verwiesen (§ 47 AVG). Diese kommen daher auch im Verwaltungsverfahren zur Anwendung.

In the case of documentary evidence as part of administrative proceedings, reference is made to the rules of the General Administrative Proceedings Act (§ 47 AVG). These rules are accordingly also applied to administrative proceedings.

3.2. Besonderheiten E-Mail

In der österreichischen Gerichtspraxis werden E-Mails grundsätzlich in ausgedruckter und somit in Papierform vorgelegt. Für diese ausgedruckten E-Mails gelten – ebenso wie für allenfalls in elektronischer Form vorgelegte – die zu Punkt 2.1 dargelegten Grundsätze.

3.2. Special aspects regarding e-mail

In Austrian legal practice, e-mails are always presented in printed form, i.e. on paper. The relevant principles set forth under item 2.1 apply to such e-mail printouts as to all e-mails in electronic form.

3.3. Beweislast des Zuganges

Wird von einer Partei im Verfahren bestritten, ein E-Mail erhalten zu haben, so handelt es sich um ein Zugangsproblem, das bei postalischer Postbeförderung aber auch per Übermittlung eines Telefaxes schon lange bekannt ist. Die diesbezüglichen Grundsätze werden auch bezüglich der Beweislast des Zuganges einer E-Mail angewendet.

Der österreichische Oberste Gerichtshof hat hiezu erst unlängst festgehalten (OGH 29.11.2007, 2 Ob 108/07g), dass die Absendung eines E-Mails keinen Anscheinsbeweis dahingehend begründet, dass der Empfänger dieses E-Mail auch erhalten hat. Es kann daher mittels eines E-Mail-Sendeprotokolls der Anscheinsbeweis des Zugangs eines E-Mails nicht erbracht werden. Erläuternd führte das Höchstgericht zum Beweis des Zugangs eines E-Mails aus, dass es dem Absender eines E-Mails möglich ist, sich den Empfang desselben auf einem sicheren Kommunikationsweg bestätigen zu lassen, durch ein den Empfang des E-Mails bestätigendes Antwortmail des Empfängers oder durch telefonische Rückfrage und anderes mehr.

3.3. Burden of proof regarding receipt

If a participant in a proceeding denies having received an e-mail, this is a problem of receipt long familiar from postal deliveries as well as facsimile communications. The principles concerning burden of proof here also apply to receiving e-mails.

In a recent ruling issued by the Austrian supreme court (OGH 29.11.2007, 2 Ob 108/07g), dispatch of an e-mail does not constitute prima facie evidence that the addressee actually received the e-mail. Consequently, submission of an e-mail transmission log does not constitute prima facie evidence of receipt of the e-mail. As regards proof of receipt of e-mails, the supreme court explained that the sender of an e-mail is able to obtain confirmation of mail receipt via a secure communication channel, e-mail response by the addressee announcing receipt of the sent mail, telephone enquiry, etc.

3.4. Haftung vermeiden

Die Verletzung der Buchführung- und/oder Aufbewahrungspflichten kann zahlreiche rechtliche Konsequenzen nach sich ziehen, die im Rahmen dieser Stellungnahme auch nicht annähernd dargestellt werden können. Lediglich zur Illustration seien jedoch einige Beispiele angeführt, dass die Verletzung derartiger Pflichten gerichtliche Straftatbestände erfüllen kann, etwa § 292 StGB (Urkundenunterdrückung) oder § 122 (GmbHG) bzw. § 255 AktG (unrichtige Wiedergabe, Verschleierung oder Verschweigung der tatsächlichen Verhältnisse oder Umstände einer Gesellschaft).

3.4. Avoidance of liability

Breach of bookkeeping and/or safekeeping obligations has numerous potential legal repercussions which cannot even be outlined in this report. Listed here purely as illustration, however, are some statutory criminal offences which can be constituted by a breach of such obligations, e.g. § 292 of the Strafgesetzbuch (Criminal Code) (suppression of documents), § 122 GmbH-Gesetz (Law Concerning Limited Liability Companies) and § 255 of the Aktiengesetz (Corporation Law) (incorrect rendering, disguising or concealment of actual company relationships or circumstances).

Weiters können Geschäftsführer oder Vorstände von Gesellschaften bei Verletzung derartiger Pflichten gegenüber der Gesellschaft schadenersatzpflichtig werden.

Kommt eine Partei in einem Zivilverfahren einem Auftrag zur Vorlage einer Urkunde nicht nach, unterliegt es der freien Beweiswürdigung des Gerichtes, ob die Angaben der Gegenpartei über den Urkundeninhalt als erwiesen anzusehen sind.

By breaching such obligations, moreover, managing directors or executive boards of companies can become liable to compensate the company for incurred damage.

If a participant in civil proceedings fails to submit an ordered document, the court at its own discretion assesses the available evidence to decide whether the opposing party's statements concerning the document's contents are valid.

France

Authors:

Philippe Martin
Associé'

Bureau van Dijk
33 rue de Naples
75008 Paris - France

Phone: +43 1 45 24 25 23

Mobile: +43 6 12 34 74 92

E-Mail: phm@bvdic.com

www.bvdic.com

Laurent Prével
Laurent Prével Conseils
E-Mail: lprevel.conseil@wanadoo.fr

Gérard Weisz
Sirius System
E-Mail: gerard.weisz@sirius-system.com

Olivier Iteanu
Avocat
E-Mail: oiteanu@iteanu.com

Présentation

L'exposé de la situation française est organisé en quatre parties:

- Présentation générale du statut des documents numériques dans le contexte général du droit français
- Précisions sur le contexte fiscal
- Précisions sur le statut et les contraintes liées à la gestion des messages électroniques
- Stockage électronique des documents financiers

1. Le contexte général du droit français

Le droit français est régi par des lois regroupées dans des codes spécifiques aux thèmes de l'action juridique. Ces codes de lois sont régulièrement complétés et précisés par des différents types de textes : décrets, arrêtés, circulaires, instructions.

Quatre codes sont particulièrement importants pour les questions relatives à la gestion des affaires :

- Le code général des impôts (CGI) dont le contenu et la portée seront traités dans la partie 2 ;

Presentation

This overview of the French situation is organized into four parts:

- A general introduction to the status of digital documents within the general context of French law
- Details concerning the fiscal context
- Details concerning the status and restrictions connected with the management of electronic messages
- Electronic Storage of Financial Documents

1. Overall French law context

French law is governed by laws which are grouped under codes specific to the subjects of the legal action. These law codes are regularly supplemented and clarified by various types of texts: decrees, orders, circulaires (a decree specifying how a law should be enforced) and directives.

Four codes are especially important for questions relating to business management:

- The Code Général des Impôts (CGI – General Tax Code), whose content and scope will be dealt with in part 2;

- LeLe code civil ;
- Le code pénal ;
- Le code de commerce.

Le statut juridique du document numérique dans le droit français est posé par la loi du 13 mars 2000 qui transpose la directive européenne N° 93 de 1999 en modifiant le code civil.

Ces modifications définissent la notion d'écrit électronique et le rôle de la signature électronique. Le code civil modifié distingue l'écrit (nativement) numérique et l'écrit sur support papier converti par numérisation produisant une copie numérique.

Les changements du code civil portent sur les points suivants.

Le document numérique comme preuve

- « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à garantir l'intégrité. »
  (art. 1316-1 Code civil)

- « L'écrit sur support électronique a la même force probante que l'écrit sur support papier. »
  (art. 1316-3 Code civil)

En cas de conflit de preuve

- « Le juge apprécie la preuve la plus vraisemblable sauf en cas de convention de preuve (réseau fermé) »
  (art. 1316-2 Code civil)

Signature électronique

La signature électronique identifie l'auteur du document et garantie l'intégrité du document. Elle est définie dans le code civil modifié :

- The Code Civil (Common Law);
- The Code Pénal (Penal Code);
- The Code de Commerce (French Company Law).

The legal status of the digital document in French law is laid down by the law of March 13, 2000 which transposes the European Directive No 93 of 1999 by modifying the code civil (common law).

These modifications define the notion of the electronic document and the role of the electronic signature. The modified Code Civil (common law) makes a distinction between a (natively) digital document and a document on paper medium converted by digitization to produce a digital copy.

The changes in the Code civil (Common Law) concern the following points.

The digital document as evidence

- "The document in electronic form is admissible as evidence in the same way as documents on paper medium, provided that the person who issued it is duly identified and that it has been drawn up and stored under such conditions as to guarantee its integrity." (article 1315-1, *Code civil* – Common Law)

- Documents in electronic media have the same probative force as documents on paper media" (article 1316-3, *Code civil* – Common Law)

Where there is a dispute over evidence

- "The judge assesses the most plausible evidence, except where there is an Agreement on evidence (closed network)"
  (Article 1316-2, Code civil – Common Law)

Electronic signature

The electronic signature identifies the author of the document and guarantees the integrity of the document. It is defined in the modified *code civil*:

- « Lorsqu'elle est électronique, elle (la signature) consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État. » (art. 1316-4 alinéa 2 Code civil)

- "When it is electronic, it (the signature) consists of the use of a reliable identification procedure that guarantees its link with the document to which it is attached. It is presumed that this process is reliable, until there is evidence to the contrary. At the time of creating the electronic signature, that the identity of the signatory is guaranteed and the integrity of the document is guaranteed, under conditions set by decree of the *Conseil d'État* (Council of State)."
(Article 1316-4, paragraph 2, *Code civil* - Common Law)

Deux types de signature sont distingués par le décret du Conseil d'État du 30 mars 2001.

A distinction is made between two types of signature by the Council of State's decree dated March 30, 2001.

- Signature simple : « une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du Code civil »
(Décret art. 1.1)

- Simple signature: "a data item which results from the use of a process meeting the conditions defined in the first sentence of the second paragraph of article 1316-4 of the *Code civil*"
(Decree Article 1.1)

- Signature sécurisée : « une signature électronique qui satisfait, en outre, aux exigences suivantes (Décret art. 1.2):
  - Être propre au signataire
  - Être créée par des moyens que le signataire puisse garder sous son contrôle exclusif
  - Garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable. »

- Secure signature: "an electronic signature which satisfies, furthermore, the following requirements
(Decree Article 1.2):
  - It must belong to the signatory
  - It must be created by means which the signatory can keep under his or her exclusive control
  - It must guarantee a link with the document to which it is attached, such that any subsequent modification of the documents can be detected."

La signature sécurisée (« signature avancée définie par la directive européenne de 1999) bénéficie d'une présomption de fiabilité.
Cette signature est utilisée par les officiers ministériels (notaires et huissiers). Sa mise en œuvre est complexe et couteuse).

The secure signature (advanced signature as defined by the European Directive of 1999) benefits from a presumption of reliability.
This type of signature is used by members of the legal profession (notaries and bailiffs). Its implementation is complex and costly.

Les actes authentiques créés par les notaires et les huissiers sont régis par des décrets publiés en 2005.

Authentic deeds created by notaries and bailiffs are governed by decrees published in 2005.

La norme française NF Z 42-013 définit les principes à respecter pour la conception et l'exploitation des systèmes informatiques capables de conserver les documents numériques dans le respect des exigences légales résumées ci-dessus.

The French standard NF-Z 42-013 defines the principles to be respected for the design and use of computer systems capable of storing digital documents in accordance with the legal requirements summarized above.

Archivage

La loi du 15 juillet 2008 rappelle que l'archivage est une obligation légale. Elle définit ce qui doit être archivé, mais ne définit pas les durées de conservation sauf dans certains cas particuliers.

Le code civil définit des durées de prescription qui constituent, de fait, des durées de conservation minimales des archives.

Les principes de gestion et d'archivage des données relatives aux personnes sont définis et contrôlés par la Commission Informatique et Liberté (Loi du 6 janvier 1978)

Archiving

The law of July 15, 2008 mentions that archiving is a legal obligation. It defines what must be stored, but does not define the retention periods, except in certain special cases.

The *Code civil* (Common Law) defines the prescription periods which constitute, de facto, the minimum file retention periods.

The principles for managing and storing data relating to individuals are defined and controlled by the French Data Protection Agency (CNIL – *Commission Nationale de l'Informatique et des Libertés*)
(Law of January 6, 1978)

En résumé, les points importants

- Les documents nativement numériques (= écrits électroniques natifs) ont le même pouvoir de preuve que les documents sur support papier à condition de garantir :
  - L'identification de leur auteur au moyen d'une signature électronique
  - L'intégrité des documents.
- La numérisation des documents créés ou reçus sur support papier produit une copie numérique qui ne se substitue pas en tant que preuve à l'original sur papier.
- De même, l'impression sur papier d'un document nativement numérique produit une copie qui n'a pas la valeur de preuve de l'original numérique.

To sum up the important points:

- Documents which are natively digital (= native electronic documents) have the same evidential power as documents on paper media, provided that they guarantee:
  - Identification of their author using an electronic signature
  - Integrity of the documents.
- Digitization of documents created or received on paper media produces a digital copy which does not substitute the paper original as evidence.
- In the same way, the printing on paper of a document which is natively digital produces a copy which does not have the evidential value of the digital original.

- Les préconisations de la norme NF Z 42-013 visent à construire des systèmes d'archivage électronique répondant aux exigences du droit français en matière de preuve. La valeur de ce référentiel sera prochainement renforcée par la mise en place d'une procédure de certification.

MAIS,

- dans la situation actuelle du droit français aucun texte n'autorise la destruction des documents originaux créés ou reçus sur support papier.

DONC, *de jure*,

les juges conservent un pouvoir final d'appréciation de la valeur de preuve des documents numériques.

2. Précisions sur le contexte fiscal

Dans le paysage réglementaire et législatif français évoqué ci-dessus, l'aspect fiscal est assez prépondérant. Le droit fiscal français repose sur de nombreux textes, principalement constitués autour de ceux-ci :

- Le code général des impôts (CGI) ;
- Le livre de procédures fiscales (LPF) ;
- Des instructions de la Direction Générale des Impôts (DGI) à travers la publication du Bulletin Officiel des Impôts (BOI).

En matière de gestion et de conservation de documents, les exigences fiscales sont assez strictes, sur des durées relativement courtes (3 à 6 ans), inférieures à celles d'usage en droit commercial (10 ans), mais il est fréquent qu'un même document relève à la fois du droit fiscal et du droit commercial.

Cette réglementation est présentée ici à propos de deux cas concrets.

- The recommendations of the French standard NF Z 42-013 aim at designing electronic storage systems which meet French law requirements in terms of evidence. The value of this reference document will shortly be strengthened by the establishment of a certification procedure.

BUT,

- in the current French law situation, there is no text which authorizes the destruction of original documents created or received on paper media.

THEREFORE, *de jure,*

judges have the final power to assess the evidential value of digital documents.

2. Details concerning the fiscal context

Fiscal matters are a dominating aspect in the French regulatory and legislative context mentioned above. French fiscal law is based on numerous texts, mainly constituted around the following:

- The *code général des impôts* (CGI – General Tax Code);
- The *livre de procédures fiscales* (LPF-Book of Fiscal Procedure);
- Directives from the DGI (Direction Générale des Impôts - French National Tax Office) through the publication of the BOI (*Bulletin Officiel des Impôts* - Official Tax Bulletin).

The fiscal requirements are quite strict regarding the management and retention of documents, for relatively short periods (3 to 6 years), which are less than those in use in commercial law (10 years), but it is often the case that the same document falls within the scope of the fiscal law and the commercial law.

An introduction to these regulations is given here, with regards to two real cases.

2.1. Les factures

En droit français, trois formes de factures sont reconnues :

- La facture sous forme papier;
- La facture sous la forme « EDI » (échange de données informatisées), en respectant les spécifications de la norme internationale EDIFACT ;
- La facture « dématérialisée », au sens fiscal, en respectant les spécifications mentionnées dans les textes définissant cette forme de facture (décrets n°2003-632 du 7 juillet 2003 & n°2002-659 du 18 juillet 2003, et BOI n°136 du 7 août 2003).

Pour la conservation des factures papier, une différence de traitement existe selon le flux, et repose sur la distinction, fondamentale en droit français, entre un original et une copie :

- La facture client : les entreprises adressent ces factures à leurs clients, elles leur transmettent donc l'original, et sont ainsi amenés à conserver des copies, qui peuvent être aussi bien sous forme papier qu'au format électronique ; ceci est énoncé dans le BOI n°4 du janvier 2007 dans le cadre d'une « mesure d'assouplissement relatif aux factures clients », qui confirme que les entreprises qui transmettent des factures sur support papier peuvent en conserver un « double électronique » ;
- La facture fournisseur : les entreprises reçoivent ces factures de leurs fournisseurs ; elles sont donc destinataires d'originaux papier, et doivent ainsi conserver ces factures sous forme papier pour pouvoir justifier de la déduction de la TVA.

Pour la conservation des factures « dématérialisées », seul un archivage électronique est admis, a priori, dans le respect de l'état de l'art, c'est-à-dire en conformité avec la Norme Française Z42-013.

2.1. Invoices

In French law, three forms of invoices are recognized:

- An invoice on paper media;
- An invoice in "EDI" (*échange de données informatisées* – exchange of computerized data) format, meeting the specifications of the international EDIFACT standard;
- The "dematerialized" invoice or "e-invoice", in the fiscal sense, meeting specifications mentioned in texts defining this form of invoice (Decrees nos. 2003-632 of July 7, 2003 & 2002-659 of July 18, 2003, and BOI no. 136 of August 7, 2003).

For the retention of paper invoices, a difference in processing exists according to their flow, and is based on the distinction, fundamental in French law, between an original and a copy:

- Customer invoice: Companies send these invoices to their customers: they therefore send them the original, and so are compelled to retain copies, which could either be on paper media or electronic format; this is set out in BOI no. 4 of January 2007 within the scope of an "easing of the restrictions relating to client invoices", which confirms that companies sending invoices on paper media may keep an "electronic copy";
- The supplier invoice: Companies receive these invoices from their suppliers: they are therefore the recipients of paper originals, and so must retain these invoices on paper media to be able to justify deduction of VAT.

Only electronic storage is acceptable for the retention of "e-invoices", a priori, in accordance with best practice - that is, in compliance with French Standard Z 42-013.

Par ailleurs, les exigences sont moins fortes lorsque les clients sont des particuliers (et non des entreprises), car, dans ce cas, la question de la déduction de la TVA ne se pose pas.

D'une manière générale, la durée de six ans est appliquée. En cas de non respect, le droit à déduction de la TVA peut être refusé, une amende de 1500 € par pièce peut être appliquée, et un redressement fiscal peut être prononcé.

2.2. La comptabilité

Accompagnant la diffusion des technologies de l'information et de la communication (TIC), le traitement des documents comptables fait l'objet de textes de référence :

- Le BOI 13 L-1-06 du 24 janvier 2006, dit « instruction pour le contrôle des comptabilités informatisées » ;
- Le livre de procédures fiscales (LPF) qui explicite l'instruction nommée ci-dessus.

Les dispositions de ces textes comportent parfois des exigences contradictoires, qu'il convient d'interpréter au cas par cas. L'approche globale consiste à :

- Adapter les exigences fiscales aux supports informatiques, en intégrant le fait que, désormais, tout document comptable est généralement créé soit sous forme électronique de façon native, soit à partir de données informatiques ;
- Exiger la présentation d'une documentation, complète, à jour, relative à l'ensemble des processus informatiques concernés, de sorte que la chaîne comptable soit accessible en toute transparence et auditable aisément ;

Furthermore, the requirements are less stringent when the clients are private individuals (and not companies), because in this case VAT deduction is not an issue.

In general, the six-year period is applied. If this is not met, the right to deduct VAT can be refused, a fine of €1,500 per document can be applied, and there can be a ruling on a tax adjustment.

2.2. Accounting

Along with the distribution of information and communication technologies (ICT), the processing of accounting documents is the subject of the following reference texts:

- BOI 13 L-1-06 of January 24, 2006, known as the "directive for the control of computerized accounting";
- The LPF (*Livre de procedures fiscales* - Book of Fiscal Procedure) which clarifies the directive mentioned above.

The provisions of these texts sometimes include contradictory requirements, and it is advisable to interpret these on a case-by-case basis. The overall approach consists of:

- Adapting fiscal requirements to computer media, by integrating the fact that, henceforth, all accounting documents are generally created either in native electronic format, or from computer data;
- The requirement to produce complete and up-to-date documentation relating to all the computer processes concerned, in a manner that the accounting trail is fully disclosed and accessible and is easily audited;

- Recommander, dans le cas d'une comptabilité informatisée, une conservation dans le format d'origine (sauf mention contraire explicite) ; cet archivage doit être assuré pendant une durée de trois années dans un mode « on-line », puis pendant trois années supplémentaires sur tout support ;
- Préconiser l'utilisation d'un horodatage fiable, afin de maintenir les règles de chronologie en matière comptable, et d'offrir la traçabilité des informations.

➔ En synthèse, les règles fiscales françaises sont contraignantes. La « dématérialisation » a tendance à simplifier les procédures et assouplir les exigences du droit français. Cependant, il convient de s'assurer, pour chaque type de document visé, si des dispositions particulières existent.

- The recommendation, in the case of computerized accounting, of retention in the original format (unless explicitly stated otherwise); this storage must be ensured for a period of three years using an "online" method, then for three additional years in any media;
- The recommendation for the use of reliable time and date stamping, in order to maintain chronology rules as far as accounting is concerned, and to give traceability of information.

➔ To sum up, French fiscal rules are restricting. "Paperless commerce" has a tendency to simplify procedures and relax the requirements of French law. However, it is advisable to check if special clauses exist for each type of document specified.

Exemples de durées de conservation obligatoire des documents comptables		
Documents à conserver	Modalités de conservation	Source officielle
Livres, registres ou pièces justificatives établis sous forme informatique	Durée totale : 6 ans : 3 ans sur support informatique + 3 ans sur support au choix de l'entreprise	Livre des procédures fiscales article L102 B
Documentation relative à l'analyse, la programmation et à l'exécution des traitements informatiques	3 ans	

Examples of mandatory retention periods for accounting documents		
Documents to be retained	Retention methods	Official source
Books, registers or receipts established in electronic format	Total period: 6 years: 3 years in computer media +3 years in the company's choice of media	*Livre des procedures fiscales* (Book of Fiscal Procedure), article L102 B
Documentation relating to the analysis, programming and execution of computer processing	3 years	

3. Précisions sur les contraintes et les enjeux liés à la gestion des messages électroniques (e-mail)

Le succès de l'e-mail a provoqué de nombreuses dérives avec, parmi les conséquences, le constat que l'adresse électronique a désormais une valeur marchande plus importante que l'adresse postale. Plus rapide et facilement routable, l'e-mail est désormais fortement exploité à des fins commerciales.

3.1. Contexte juridique

Le développement de l'utilisation de la messagerie dans les entreprises soulève de nombreuses difficultés. Il en est ainsi de l'utilisation, par l'employé, de l'e-mail depuis la messagerie professionnelle. Le matériel informatique mis à disposition de l'employé est considéré comme un outil de travail et de ce fait l'employeur peut exercer un droit de regard sur les e-mails émis et reçus sur le lieu de travail d'autant que celui-ci est également aujourd'hui un facteur d'augmentation d'exposition des entreprises à des risques juridiques.

3.1.1. Utilisation des messageries dans un contexte professionnel

En droit français, l'employeur est de plein droit responsable de l'activité de ses employés. Dans le cas de l'e-mail, cela signifie que l'employeur est responsable des informations véhiculées dans ou vers l'extérieur de son entreprise. L'adresse mail professionnelle est une adresse fonctionnelle et non personnelle ce qui signifie que dès la réception d'un message, l'employé n'en est pas personnellement le destinataire, le réel destinataire est l'entreprise. Lorsqu'un employé émet ou reçoit un e-mail, le destinataire ou l'émetteur est en réalité l'entreprise. Dans ce cas, il paraît légitime que l'employeur puisse prendre connaissance du contenu des messages, émis ou reçus depuis la messagerie professionnelle, puisque ceux-ci sont censés ne contenir que des informations relatives à l'activité de l'entreprise.

3. Details of the restrictions and issues connected with managing electronic messages (e-mail)

The success of e-mail has given rise to many abuses, whose consequences include the acknowledgement that an electronic address now has a greater market value than a postal address. Fast and easily routed, e-mail is now seriously used for commercial ends.

3.1. Legal context

The development of the use of messaging systems in companies has given rise to numerous difficulties. This is the case with the use, by a staff member, of their office e-mail system. Computer system which is at the disposal of the staff member is considered to be a work tool, and for this reason the employer can exercise a right to inspect e-mail sent and received at the workplace, all the more so because this is now also a factor in the increase of companies' exposure to legal risks.

3.1.1. Use of e-mail systems in a work context

In French law, employers are automatically responsible for the work activities of their employees. In the case of e-mail, this means that employers are responsible for information conveyed internally or externally from their companies. The work e-mail address is a functional address and is not personal, which means that once a message is received, the employee is not personally the recipient - the real recipient is the company. When a member of staff sends or receives an e-mail, the recipient or the sender is in fact the company. In this case, it would appear legitimate that the employer should be aware of the contents of messages sent or received by the workplace e-mail system, since these are only supposed to contain information relating to the company's business activity.

Ainsi, l'employeur est tenu pour responsable et ce, quel que soit le contenu du message : informations qui engagent l'entreprise, injures, virus ou encore diffusion d'information confidentielle.

C'est pourquoi l'employeur peut être amené à contrôler des messages lorsque les volumes sont trop importants, pour des raisons légales ou encore pour s'assurer qu'il n'y a pas de divulgation d'informations mettant en cause la sécurité de l'entreprise ou portant atteinte à la réputation et/ou à l'image de marque de l'entreprise. Quel que soit le sens du message véhiculé dans chaque e-mail, son contenu représente toujours l'entreprise émettrice.

L'élaboration de règles ou bonnes pratiques de l'utilisation de la messagerie dans l'environnement professionnel permet de tenir au courant les employés des risques encourus par le simple envoi d'un e-mail et d'atténuer les éventuelles conséquences juridiques pour l'entreprise. Ces dispositions peuvent prendre diverses formes : clauses dans les contrats des employés, charte e-mail ou articles du règlement intérieur. Elles ont pour objectif d'exposer les règles à suivre en matière de traitement des e-mails professionnels mais aussi personnels.

Therefore, the employer is held responsible, whatever the content of the message, for information which is binding on the company, abuse, viruses or dissemination of confidential information.

This is why the employer can be forced to check messages when volumes are too high, for legal reasons or to ensure that no information that would implicate the company's security or that is damaging to the reputation and/or the image of the company's brand is disclosed .Whatever the meaning of the message conveyed in each e-mail, its contents always represent the company who issued it

Drawing up rules or good practices for the use of the e-mail system in the workplace allows employees to be kept aware of the risks incurred by the simple sending of an e-mail and to reduce the potential legal consequences for the company. These provisions may take various forms: clauses in employee contracts, an e-mail charter or internal policy and procedure articles. The aim of these articles is to set out the rules to be followed regarding the processing of workplace and also personal e-mails.

3.1.2. Secret de la correspondance

Rien n'interdit pas l'usage de la messagerie professionnelle à des fins personnelles. En théorie, l'employé ne devrait en avoir qu'un usage professionnel, mais rien ne l'empêche d'en avoir un usage privé.

Un des problèmes principaux de l'e-mail est sa nature juridique dans la mesure où aucun texte ne le vise directement. On peut donc légitimement s'interroger sur l'application du secret des correspondances aux e-mails échangés à partir des messageries professionnelles. Si l'employeur est en droit de disposer d'un accès aux e-mails de ses collaborateurs étant donnés les risques qui pèsent sur l'entreprise, dans les textes il en est tout autrement.

3.1.2. Secrecy of correspondence

There is nothing which prohibits the use of the workplace e-mail system for personal purposes. In theory, staff members should only use it for work matters, but nothing prevents employees from using it for private purpose.

One of the main issues of e-mail is its legal nature, considering that there is no law which deals with it directly. The application of secrecy of correspondence by e-mail exchanged using workplace e-mail systems might therefore legitimately be questioned. If employers have the right to access their employees e-mails, given the risks ensuing for the company, it is completely different within law texts.

La prise de connaissance du contenu d'un e-mail sert à contrôler l'employé et ce contrôle ne peut se faire que selon les règles du droit du travail.

Ainsi, l'e-mail est assujetti, de la même manière qu'un courrier papier, au secret des correspondances. Les correspondances privées sont protégées par la loi et de fait, l'employeur ne peut opérer de contrôle sur celles-ci. Il n'a pas le droit de prendre connaissance du contenu des messages émis et reçus par l'employé et même lorsqu'il a interdit une utilisation personnelle de la messagerie professionnelle.

Being aware of the contents of an e-mail is a means of controlling the employee, and this control can only be carried out according to the employment law regulations.

Therefore the e-mail is subject, in the same way as a paper letter, to secrecy of correspondence. Private correspondence is protected by law and de facto the employer cannot exercise any control over this. The employer does not have the right to know the contents of the messages sent and received by the employee, even when personal use of the workplace e-mail system is prohibited by the employer.

3.1.3. La valeur probante des e-mails

Du point de vue juridique, une entreprise - une organisation ou tout individu peut être tenue responsable du contenu d'un e-mail. Un e-mail peut permettre de prouver en justice lorsque la loi admet la preuve par tout moyen (notamment en Droit commercial). Ainsi, la conservation des e-mails devient un impératif d'autant que celle-ci est reconnue depuis la LCEN n°2004-575 du 21 juin 2004 loi pour la confiance dans l'économie numérique qui transpose la directive européenne 2000/31/CE. Le texte stipule que les écrits exigés pour la validité d'un acte juridique peuvent être établis et conservés sous forme électronique ce qui signifie que la valeur d'un « original » sous forme électronique est désormais reconnue.

3.1.3. The evidence value of e-mails

From a legal standpoint, a company, an organization or any individual may be held responsible for the content of an e-mail. An e-mail can be used as proof in court when the law accepts evidence by any means (in particular in Commercial law). In this way, the retention of e-mails becomes imperative in so far as it has been recognized since the LCEN (*Loi sur la Confiance dans l'Economie Numérique* - Law on the Confidence in The Digital Economy) no 2004-575 of June 21, 2004, which transposes the European directive 2000/31/CE. The text states that documents required for the validity of a deed can be drawn up and kept in electronic format, which means that the value of an "original" in electronic format is now recognized.

La messagerie électronique s'étant imposé comme moyen de communication le plus utilisé au sein des entreprises, il en résulte l'obligation pour celle-ci de gérer et d'archiver les e-mails pour préserver des données sensibles de l'activité de l'entreprise.

As the electronic messaging system becomes the most used means of communication within companies, there is a resulting obligation for the latter to manage and store e-mails in order to keep data which is sensitive to the company's business activity.

L'archivage électronique des mails dans les entreprises doit prendre en compte la problématique d'une volumétrie importante et difficilement maîtrisable sans oublier qu'il est difficile de juger de la valeur d'un e-mail et de son utilité postérieure.

Electronic storage of e-mails within the companies must take into account the issue of a significant volume of data which is difficult to control, without forgetting that it is difficult to assess the value of an e-mail and its subsequent usefulness.

En outre, l'assujettissement des e-mails au secret des correspondances, même dans le cadre professionnel, démontre un vide juridique concernant la reconnaissance des e-mails à caractère strictement professionnel et implique un certain nombre de contraintes sociales qui ne facilitent pas la mise en place de ce type de projet.

3.1.4. Conformité à la directive européenne

En avril 2008, l'Union européenne a décidée d'adopter une directive, inspirée de la loi américaine (Sarbannes-Oxley), appelée EuroSOX qui s'applique dès 2009.

A l'image des Etats-Unis, toutes les entreprises cotées aux marchés boursiers européens sont concernées. Cette nouvelle réglementation européenne implique une nouvelle gestion technique et organisationnelle des documents. Pour répondre aux exigences de conformité de celle-ci, chaque entreprise va être dans l'obligation de mettre en place des dispositifs tels que l'archivage des e-mails et ainsi réduire leurs risques d'exposition.

Dans un contexte de globalisation, même si la réglementation française n'impose pas encore l'archivage des e-mails, les entreprises doivent se conformer aux législations des autres pays dès lors qu'elles y exercent une activité ou y investissent. En outre, les préconisations de la communauté européenne concernant l'archivage des e-mails des entreprises de plus de 50 salariés et la récente adoption de l'EuroSOX vont fortement contribuer à renforcer cette obligation. Les entreprises doivent désormais se préparer à être capables de restituer de façon fiable et rapide toutes les pièces légales pour répondre à des impératifs légaux.

Furthermore, subjecting e-mails to correspondence secrecy, even within the scope of the workplace, shows that there is a legal loophole concerning the recognition of e-mails of a strictly professional nature and involves a certain number of social restrictions, which do not facilitate the implementation of this type of project.

3.1.4. Compliance with the European directive

In April 2008, the European Union decided to adopt a directive, inspired by American law (Sarbannes-Oxley), called EuroSOX, which is applicable since 2009.

Following the US model, all companies quoted on the European stock exchanges are affected. This new European regulation involves a new technical and organizational management of documents. To meet the requirements for complying with this, each company will have to implement devices such as e-mails archiving system, and therefore reduce their exposure to risks.

Within a context of globalization, even if French regulations do not yet impose the archiving of e-mails, companies must conform to the legislation of other countries where they are carrying out a business activity or making investments. Furthermore, the recommendations of the European Community concerning archiving of e-mails for companies with more than 50 staff members and the recent adoption of EuroSOX will make a strong contribution to reinforcing this obligation. Companies must now be prepared to be able to restore all legal documents in a fast and reliable way to meet legal requirements.

3.1.5. Préserver les données à caractère personnel

La Commission nationale de l'informatique et des libertés a également publié une délibération en octobre 2005 portant adoption d'une recommandation sur les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel. Elle préconise notamment l'attribution de durées de conservation selon les données traitées et un contrôle de l'accès et de la diffusion de ces données, l'utilisation de procédés d'anonymisation.

3.1.5. The storage of personal data

The *Commission nationale de l'informatique et des libertés* (French National Data Protection Agency) in October 2005 also published a decision dealing with electronic archiving of personal data within the private sector. In particular, it recommended to adjust the retention periods according to the data being processed and control of access to and distribution of this data, and the use of procedures for masking sensitive information.

3.2. Les enjeux liés à l'archivage des e-mails

3.2. Issues related to e-mails archiving

3.2.1. Gérer l'accroissement des volumes

Les e-mails émis par les entreprises représentent près des deux tiers des e-mails qui circulent chaque jour dans le monde. Ils sont la première cause de l'augmentation des espaces de stockage en entreprise. Selon une étude, le nombre de messages reçus par jour par employé est évalué à 133 (Source Radicati Group Dec. 2007) dans les entreprises et estimés à 166 en 2009 nécessitant 21,3 Mo de capacité de stockage quotidienne. De fait, les coûts de stockage représentent entre 15 et 25% des budgets informatiques.

3.2.1. Managing the growth in volume

E-mails sent by companies represent almost two thirds of the e-mails circulating daily in the world. They are the main cause of the increase in storage space within a company. According to one study, the number of messages received per day per employee is assessed at 133 (source: Radicati Group Dec. 2007) within companies and is estimated to be 166 in 2009 requiring 21.3 Mb of storage daily. In fact, storage costs represent between 15 and 25% of IT budgets.

3.2.2. Retrouver efficacement les messages

L'archivage des e-mails doit être conçu de façon centralisée sans avoir recours à la sauvegarde des fichiers natifs de la messagerie de chaque employé afin de sécuriser et préserver les documents des pannes assez fréquentes sur les postes utilisateurs.

3.2.2. Finding messages efficiently

The storage of e-mails must be designed in a centralized way without having to save the native messaging system files for each employee, in order to secure and protect documents from fairly frequent crashes on user workstations.

Ces dispositions permettent de réduire le risque global pour les entreprises de perte d'informations en centralisant le stockage du contenu des messageries y compris les fichiers.

La centralisation du stockage des e-mails dans un ou plusieurs conteneurs à accès rapide et un outil de recherche performant permettent de favoriser le partage des informations mais surtout de retrouver plus facilement une information noyée dans la masse et permet une récupération rapide d'e-mails spécifiques via des requêtes afin de répondre aux obligations récentes en matière de restitution de preuve.

3.2.3. Responsabiliser les utilisateurs

Le besoin de responsabiliser les utilisateurs provient du fait que ce sont eux qui sont les détenteurs des e-mails et des informations qu'ils contiennent dans la mesure où c'est chaque utilisateur qui gère sa messagerie. Le facteur humain dans la gestion des e-mails est donc essentiel.

La mise en place d'une solution d'archivage doit permettre aux utilisateurs de faciliter la gestion de leurs messageries tout en réduisant le temps qui leur est consacré. Cependant, des règles de gestion doivent être définies, en respectant les habitudes des collaborateurs, et que ceux-ci devront appliquer pour faire un usage optimal du processus d'archivage. Elles doivent également respecter leurs méthodes de travail.

3.2.4. Intégrer la politique globale de conservation des informations

L'e-mail doit donc être intégré dans la réflexion sur l'organisation et le traitement de l'information et plus spécifiquement des documents. Actuellement, alors que le courrier papier fait l'objet d'un processus de traitement (distribution, ouverture, diffusion, traitement et conservation), les e-mails sont, dans le meilleur des cas, conservés par le ou les destinataires sans nécessairement faire l'objet d'un classement et d'un archivage réglementé.

These provisions allow reducing the overall risk for companies regarding loss of information by centralizing the storage of e-mail system content, including files.

Centralization of e-mail storage in one or more rapid-access container applications and a high-performance search tool favors information sharing, but also allows a piece of information buried in the mass to be found more easily and allows rapid restoring of specific e-mails on request in order to respond to the recent obligations regarding restitution of evidence.

3.2.3. Give users a sense of responsibility

The need to give users a sense of responsibility stems from the fact that it is they who are the keepers of the e-mails and the information which they contain, in so far as each user is the one who manages his own e-mail. The human factor in the management of e-mails is therefore essential.

Implementation of a storage solution must allow users to facilitate the management of their e-mail whilst reducing the time they spend on this task. However, management rules must be defined whilst respecting colleagues' usual working practices, and that these must apply to make optimal usage of the storage process. They must also respect their working methods.

3.2.4. Integrate the overall information storage policy

E-mail must therefore be integrated into any considerations regarding the organization and processing of information and more specifically of documents. Currently, while paper mail is subject to a processing procedure (distribution, opening, dissemination, processing and storage), e-mails are in the majority of cases kept by the recipient(s) without necessarily being subject to a regulated classification and filing system.

Comme pour tous les documents contenant des informations sensibles, l'archivage des emails doit être envisagé car il devient stratégique dès lors que l'entreprise est amenée à prouver la trace d'un envoi ou la réception d'un e-mail, ou encore à attester une date ou un contenu.

3.2.5. Identifier le ROI (retour sur investissement)

Du point de vue de la productivité, l'archivage permet de réduire le temps accordé à la gestion des e-mails que ce soit pour les utilisateurs et le service informatique de l'entreprise.

Ainsi le collaborateur n'a plus à se soucier de trier, vider, sauvegarder et archiver régulièrement sa messagerie lorsque celle-ci est saturée.

De même, les services informatiques réduisent leurs démarches personnelles auprès des utilisateurs pour effectuer des sauvegardes des messageries ou de restitution d'e-mails. En outre, la recherche et la restitution d'un e-mail sont facilitées par la centralisation des informations et un outil de recherche.

Du point de vue réglementaire, le bénéfice pour l'entreprise est d'être conforme à la législation. En mettant en place un archivage des e-mails, l'entreprise s'assure, en cas de litige ou de contrôle, de pouvoir fournir toutes les pièces nécessaires. Si l'on peut évaluer approximativement le coût de stockage induit par l'archivage, on peut également mesurer celui de la perte d'un e-mail stratégique.

Dans le cas d'un non-respect des directives et textes légaux, l'entreprise ne pourrait éviter les procès perdus et les sanctions financières. Elle risquerait, en sus, de nuire à sa réputation et à son image de marque si ce non-respect au règlement venait à être connu de sa clientèle et du public.

As for all documents containing sensitive information, the filing of e-mails must be considered because it becomes strategic when the company is induced to prove an e-mail send-and-receipt trail, or to confirm a date or content.

3.2.5. Identifying ROI (return on investment)

From the standpoint of productivity, storage allows the time allocated for managing e-mails to be reduced, whether this is for the users or the company's computing department.

In this way, the staff member does not have to worry about sorting, saving and regularly archiving his or her inbox when it gets full.

In the same way, IT services reduce their own involvement with users to carry out backup operations of mailboxes or e-mails recovery. Furthermore, the search and recovery of an e-mail is eased by centralizing information and by using powerful search tool.

From a regulatory point of view, the benefit to the company is to comply with regulations. By implementing e-mail archiving, the company ensures, in case of litigation or inspection, that they are able to provide all the required documents. If the cost of storage induced as a result of archiving can be assessed, the cost of the loss of a strategic e-mail can also be estimated.

If directives and legal texts are not respected, the company cannot avoid lost lawsuits and financial sanctions. In addition, it would risk damaging its reputation and its brand image if this non-respect of regulation came to the attention of its clientele and the public.

3.3. Conclusion

Le cadre juridique français pour la gestion des e-mails est encore limité voire inexistant dans la mesure où l'e-mail est pour le moment assimilé à un courrier « traditionnel ».

Les caractéristiques propres aux e-mails telles que le transport de pièces jointes modifiables, le transfert vers d'autres adresses, l'empilement de messages sont autant de sources de litiges éventuels dont le droit devra tenir compte notamment dans le cadre de la valeur probatoire des messages électroniques.

D'autre part, au même titre que le courrier traditionnel peut être expédié sous forme de lettre recommandée avec demande d'avis de réception (LRAR), il devient nécessaire de disposer d'un texte qui permette de reconnaître le recommandé électronique en alternative à la LRAR sous réserve de dispositions techniques permettant d'assurer la fiabilité technique de celui-ci.
Pour être efficace et rentable une solution d'archivage d'e-mails doit être conçue pour permettre :

- de gérer la volumétrie et sa croissance,
- de protéger les données critiques,
- d'améliorer la productivité des utilisateurs,
- de garder une mémoire informationnelle de l'entreprise
- d'être en conformité avec la législation et la réglementation.

4. Stockage électronique des documents financiers

En principe, les contraintes légales pour le stockage électronique des documents financiers sont les mêmes que les documents soient stockés en France, dans un pays de l'Union Européenne ou dans un pays tiers.

Dans tous les cas, l'entreprise doit être capable de présenter les documents conservés sous forme électronique sur un support standard.

3.3. Conclusion

The French legal framework for managing e-mails is still limited, or even non-existent, in so far as an e-mail is for the moment categorized to be the same as "traditional" mail.

Email properties, such as the sending of modifiable attachments, forwarding, and message histories are all sources of potential litigation which should be taken into account by the law, particularly within the scope of the evidential value of electronic messages.

On the other hand, in the same way that traditional mail can be sent in the form of registered letter with a request for acknowledgement of receipt (LRAR - lettre recommandée avec demande d'avis de réception), it becomes necessary to be provided with a text which allows electronic registration as an alternative to the registered letter, subject to technical clauses allowing the technical reliability of this to be ensured.
To be efficient and profitable, an e-mail archiving solution must be designed to allow:

- Management of volume and its growth,
- Protection of critical data,
- Improvement in user productivity,
- Preservation of a computerized memory for the company
- Conformity with the legislation and regulations.

4. Electronic storage of financial documents

In principle, the legal requirements for the electronic storage of financial documents are the same whether said documents are stored in France, in the European Union or outside the European Union.

Any way, the Company should be able to produce the stored documents at any time on a standard electronic support.

De plus, l'entreprise doit présenter une description détaillée et à jour du système de stockage électronique utilisé afin de permettre aux autorités concernées d'auditer le système et les modalités de stockage des documents (notamment la sécurité et la fiabilité du système).

In addition, it must keep a detailed and updated description of the electronic storage system in order to enable the concerned authorities to check the system and know how the documents are stored (eg to check the security / reliability of the storage system).

D'autre part, il est important de s'assurer que les documents financiers archivés ne contiennent pas de données particulières entrant dans le champ de la protection des données relatives aux personnes.

Besides, it is important to ensure that financial documents do not contain certain data which are subject to specific protection rules such as "Personal Data".

En fait, tous les traitements informatiques de données personnelles **doivent être déclarés** à la CNIL (Commission Nationale Informatique et Libertés – www.cnil.fr).

In fact, each Personal Data Processing (PDP) must be **declared** to the CNIL (French authority in charge of personal data protection).

De plus, le transfert des données personnelles en dehors de l'Union Européenne est réglementé par les dispositions de la loi informatique et liberté (Loi n° 78-17 du 6 janvier 1978) dont l'article 68 stipule :

In addition, the transfer of personal data outside the European Union is governed by the legal provisions of the French personal-data protection act (French Act n° 78-17 dated January 6th 1978) which states in Article 68:

« Le responsable d'un traitement informatique **ne doit pas** transférer de données personnelles dans un Etat en dehors de l'Union Européenne si l'Etat ne garantit pas un niveau de protection adéquat vis-à-vis de la protection de la vie privée et des droits fondamentaux par rapport aux traitements informatiques des données »

« The responsible of the data processing **can not** transfer personal data to a State outside the European Union if that State does not provide an adequate level of protection of privacy and fundamental rights with regard to data processing »

Cet article est l'application de l'article 25 de la Directive Européenne 95-46 EC « Directive sur la protection des données »

Said article is the application of article 25 of the EU Directive 95-46/EC – « *The Data Protection Directive* » :

« *Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.* »

« *The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.* »

La Commission Européenne a été autorisée par le Parlement Européen à décider qu'un pays tiers fournit un niveau de protection des données personnelles équivalent à celui de l'Union Européenne.

The European Commission has been authorized by the European Parliament to make decisions stating that a third country is providing a protection level of personal data equivalent to that of the European Union.

Par conséquent, si si la Commission Européenne considère qu'un pays tiers fournit un niveau de protection des données personnelles équivalent à celui de l'Union Européenne, il n'est pas nécessaire d'obtenir une autorisation pour transférer des données personnelles dans le pays considéré.

A notre connaissance, la Commission Européenne a déjà pris une décision favorable concernant les pays suivants :

- Argentine
- Canada (seulement pour le transfert des données vers des entreprises soumises à la loi Fédérale du Canada)
- L'Ile de Man
- Jersey
- Guernesey
- USA (seulement pour les entreprises ayant signé le « Safe Harbour Agreement »

Par conséquent, nous pouvons distinguer trois situations :

1 - Transfert de documents financiers contenant des données personnelles vers un Etat membre de l'Union Européenne

Il n'est pas nécessaire d'obtenir une autorisation pour stocker les documents dans un Etat quelconque de l'Union Européenne (cependant, le transfert doit être mentionné dans la déclaration du traitement informatique envoyée à la CNIL)

2 - Transfert de documents financiers contenant des données personnelles vers un pays tiers considéré par la Commission Européenne comme fournissant un niveau de protection des données personnelles équivalent à celui de l'Union Européenne.

Il n'est pas nécessaire d'obtenir une autorisation pour stocker les documents dans le pays considéré.

Accordingly, if the European Commission considers that a third country is providing a protection level of personal data equivalent to that of the European Union, there is no need to obtain an authorization in order to transfer personal data to said country.

To the best of our knowledge, the European Commission has already made favorable decisions regarding the following countries :

- Argentina
- Canada (only for transfer to commercial companies submitted to the Canadian Federal law)
- Le Man Island
- Jersey
- Guernsey
- U.S.A. (only for companies who signed the « Safe Harbor » Agreement).

Consequently, we can distinguish three situations:

1 - Transfer of financial documents containing personal data to a member state of the European Union:

There is no need to obtain an authorization in order to store the documents in any member state of the European Union (however, the transfer must be mentioned in the data processing statement sent to the CNIL)

2 - Transfer of financial documents containing personal data to a third country considered by the European Commission as providing a protection level of personal data equivalent to that of the European Union.

There is no need to obtain an authorization in order to store the documents in said country.

3 - Transfert de documents financiers contenant des données personnelles vers un pays tiers qui n'est pas considéré par la Commission Européenne comme fournissant un niveau de protection des données personnelles équivalent à celui de l'Union Européenne.

Dans ce cas, il est nécessaire d'obtenir une autorisation spécifique de la CNIL pour procéder au transfert et au stockage des documents dans le pays considéré. Le contrat avec le prestataire assurant le stockage doit contenir des clauses spécifiques pour garantir la protection des données personnelles. Ces clauses doivent être approuvées par la CNIL.

3 - Transfer of financial documents containing personal data to a third country which is not considered by the European Commission as providing a protection level of personal data equivalent to that of the European Union.

In this case, it is necessary to obtain a specific authorization from CNIL in order to proceed with the transfer of the documents to said country (store the document in this country). The contract with the storage provider must contains specific provisions in order to insure the protection of the personal data. Said provisions must be approved by the CNIL.

Germany

Author:

Stefan Groß
Tax Attorney
Certified Information System Auditor (CISA)

Internet: http://www.psp.eu

1. Steuerrechtliche Aspekte

1.1. Aufbewahrungsform

Steuerrecht und Handelsrecht gestatten über § 147 Absatz 2 AO, § 257 Absatz 3 HGB im Grundsatz, die Aufbewahrung von Unterlagen auf einem Bild- oder anderen Datenträger, wenn dies in Grundsätzen ordnungsmäßiger Buchführung (GOB) entspricht. Bezogen auf das Steuerrecht gilt, dass die Wiedergabe oder die Daten mit den empfangenen **Handels- und Geschäftsbriefen** und den **Buchungsbelegen** bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen müssen, wenn sie lesbar gemacht werden.

Soweit die entsprechenden Unterlagen mit Hilfe eines Datenverarbeitungssystems erstellt worden sind, besteht auf der Grundlage des § 147 Absatz 6 AO, ein elektronisches Zugriffs- und Auswertungsrecht für den Betriebsprüfer. Hier verlangt das Steuerrecht, dass die **Daten** über die Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht werden können und maschinell auswertbar sind. Für das Datenzugriffsrecht (**GDPdU**) gilt der Grundsatz, dass originär digitale Unterlagen auf maschinell verwertbaren Datenträgern zu archivieren sind. Diese dürfen mithin nicht ausschließlich in ausgedruckter Form aufbewahrt werden, sondern sind auf Medien zu archivieren, die eine maschinelle Auswertung zulassen.

1. Fiscal aspects

1.1. Storage format

Under § 147 Paragraph 2 of the German Tax Code (Abgabenordnung – AO), and § 257 Paragraph 3 of the German Commercial Code (Handelsgesetzbuch - HGB) tax law and trade law in principle allow documents to be stored on an image or other data carrier if this complies with German generally accepted accounting principles (Grundsätze ordnungsmäßiger Buchführung - GOB). With regard to tax law, the reproduction or data must be visually identical to the **commercial and business correspondence** and **accounting documents** and must be identical to the other documents in terms of content when they are made readable.

If the documents were created using a data processing system, the tax auditor has a right under § 147 Paragraph 6 AO to access and evaluate them electronically. In this case, tax law demands that the data remain available at all times during the retention period, that the data can be made immediately readable and that the data can be evaluated by computer . With regard to the right to access data (**GDPdU - principles for data access and verifiability of digital documents**), the principle is that documents originally created digitally must be archived on data carriers that can be evaluated by computer. These may therefore not be stored exclusively in printed form, but must be archived on media that allow computer evaluation.

1.2. Aufbewahrungsfristen

Maßgeblich für die steuerlichen Aufzeichnungs- und Aufbewahrungspflichten in Deutschland ist die Abgabenordnung (AO). Entsprechend § 147 Abs. 1 AO sind Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen sowie Buchungsbelege 10 Jahre aufzubewahren. Für empfangenen Handels- oder Geschäftsbriefe, Wiedergaben der abgesandten Handels- oder Geschäftsbriefe sowie sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind, gilt eine 6-jährige Aufbewahrungspflicht. Für Rechnungen sieht das Umsatzsteuergesetz eine eigenständige Aufbewahrungsvorschrift vor (§ 14 b UStG). Demnach hat der Unternehmer ein Doppel der Rechnung sowie alle Rechnungen, die er erhalten oder die ein Leistungsempfänger oder ein Dritter in dessen Namen für dessen Rechnung ausgestellt hat, 10 Jahre aufzubewahren.

1.2. Retention periods

The German Tax Code (AO) is the main authority on fiscal record-keeping and retention obligations in Germany. Under § 147 Paragraph 1 AO, books and records, inventories, annual financial statements, annual reports, opening balance sheets and the instructions required for reading them along with other organizational documents and accounting documents must be kept for 10 years. Commercial and business correspondence received, reproductions of commercial and business correspondence sent as well as other documents, insofar as these are important for taxation purposes, must be kept for 6 years. For invoices, the Value Added Tax Act (Umsatzsteuergesetz – UstG) stipulates a separate storage period (§ 14 b UStG). According to this provision, the business owner must keep a duplicate of the invoice plus all invoices that he has received or which the recipient of a service or a third party has issued in his name under his invoice for 10 years.

1.3. E-Mails

Bei der Qualifizierung steuerlich relevanter Daten sind insbesondere E-mails und deren Abgrenzung in der Diskussion. Gerade hier stellt sich die entscheidende Frage, ob die elektronische Post steuerrelevante Informationen zum Gegenstand hat. Auch Mitteilungen, die auf elektronischem Weg übermittelt werden, können Steuerrelevanz besitzen und damit zum sachlichen Umfang einer Außenprüfung rechnen. Aus steuerlicher Sicht sind E-mails aufbewahrungspflichtig, wenn sie Aufzeichnungen oder Geschäftsbriefe darstellen bzw. sonstige steuerlich relevante Informationen enthalten und damit für die steuerliche Sachverhaltsermittlung von Bedeutung sind. Auf der Grundlage der Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (**GoBS**) ist die elektronische Post durch Übertragung der Inhalts- und Formatierungsdaten auf einem Datenträger zu archivieren und mit einem unveränderbaren Index zu versehen, unter welchem sie bearbeitet und verwaltet wird.

1.3. E-mails

With regard to qualification as tax-relevant data, e-mails in particular and their classification are still under discussion. The crucial question is whether an e-mail contains tax-relevant information. Information transmitted by electronic means can be relevant for tax and therefore by its nature falls within the scope of a tax audit. From a tax point of view, e-mails must be retained if they represent records or business correspondence or contain other tax-relevant information and are therefore important for determining the facts for tax purposes. On the basis of the principles of generally accepted computer-assisted accounting systems (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme **- GoBS**), electronic mail must be archived by transferring the content and formatting data on to a data carrier together with an non-modifiable index, under which it will be processed and administered.

1.4. Elektronische Rechnungen

Einen Sonderfall stellen elektronische Rechnungen (Electronic Invoicing) dar, die auf der Grundlage des § 14 Absatz 3 UStG insbesondere einer qualifiziert elektronischen Signatur bedürfen. Die elektronische Version enthält in diesen Fällen gegenüber dem ausgedruckten Beleg eine Mehrinformation, für die entsprechende Aufbewahrungs- und Prüfbarkeitsvorschriften zur Anwendung kommen. Insoweit werden an die elektronische Rechnung neben den ohnehin bestehenden umfangreichen Rechnungsanforderungen des Umsatzsteuergesetzes erhöhte Anforderungen gestellt, welche bei Missachtung dazu führen, dass die übermittelten Dokumente nicht als Rechnungen gelten und der Vorsteuerabzug gefährdet ist. Daneben existieren spezifische Prüfungsvoraussetzungen nach den GDPdU, welche eine elektronische Aufbewahrung zwingend voraussetzen.

(Hinweis: Der Entwurf eines Steuervereinfachungsgesetzes 2011 sieht Vereinfachungen beim elektronischen Rechnungsversand vor, die nach derzeitigem Stand zum 1. Juli 2011 in Kraft treten sollen. Allerdings ist davon auszugehen, dass unabhängig die maßgeblichen Aufbewahrungsvorschriften unverändert erhalten bleiben.)

1.4. Electronic invoices

Electronic invoicing constitutes a special case, which requires a qualified electronic signature on the basis of §14 Paragraph 3 of the Value Added Tax Act (UStG). In these cases, the electronic version contains additional information not contained in the printed document and the relevant retention and audit rules apply to such information. The electronic invoice is subject to stricter requirements over and above the already extensive invoicing requirements of the VAT Act. If these requirements are not met, the documents transmitted may not be treated as valid invoices, which compromises the input tax deduction. Moreover, specific auditing requirements exist under the GDPdU, which demand mandatory electronic storage.

(Note: The draft version of a simplified tax law for 2011 includes simplifications to the process of electronic billing; the bill is due to become law on July 1, 2011. However, it must be assumed that the existing regulations on storage and retention will continue to apply independently of this procedure.)

1.5. Vernichtung von Originalbelegen

Immer mehr Unternehmen gehen aus Effizienz- und Kostenüberlegungen dazu über, ihre papierbasierten Dokumente einzuscannen und anschließend zu vernichten. So muss insbesondere für Zwecke des Vorsteuerabzugs, welcher auf der Grundlage des § 15 Abs. 1 Satz 1 Nr. 1 Satz 2 UStG den Besitz einer nach §§ 14, 14a UStG ausgestellten **Rechnung** verlangt, sichergestellt sein, dass das elektronische Pendant eine dem Original gleichgestellte und hinsichtlich der damit verbundenen Rechtsverbindlichkeit identische Rolle einnimmt. Von besonderem Interesse ist hier das BMF-Schreiben vom 29.1.2004, welches explizit zu den Voraussetzungen der Vernichtung von Originalbelegen aus umsatzsteuerlicher Sicht Stellung nimmt.

1.5. Destruction of original documents

For reasons of cost and efficiency, companies are increasingly scanning their paper-based documents and then destroying them. It must therefore be ensured, especially for the purposes of input tax deduction (Vorsteuerabzug), which on the basis of § 15 Para. 1 Clause 1 No. 1 sentence 2 UStG demands the possession of an **invoice** issued under §§ 14, 14a UStG, that the electronic counterpart plays a role that is equivalent and identical in terms of its legally binding force to that of the original document. Of particular interest here is the administrative directive of the German Federal Ministry of Finance (BMF-Schreiben) of January 29, 2004, which explicitly comments on the conditions under which original documents may be destroyed from a VAT perspective.

Zusammengefasst gilt: eine Papierrechnung kann unter Wahrung des Vorsteuerabzugs grundsätzlich eingescannt und anschließend vernichtet werden, wenn das Erfassungs- und Archivierungsverfahren den **GoBS** entspricht.

Briefly, it states that a paper invoice may generally be scanned and then destroyed in compliance with input tax deduction rules if the scanning and archiving procedure meets the accepted rules relating to data processing-assisted accounting systems (**GoBS**).

2. Zivilrechtliche Aspekte

2. Civil law aspects

2.1. Beweismittelkraft elektronischer Dokumente im Vergleich

In einem Gerichtsprozess ist der Beweiswert von entscheidender Bedeutung. Im Rahmen einer grundsätzlich freien Beweiswürdigung kann ein Richter nach seiner eigenen Überzeugung entscheiden, ob er einem Beweismittel Glauben schenkt oder nicht, soweit diese Beweiswürdigung mit nachprüfbaren Argumenten begründet wird. Dies gilt nicht nur für Zeugenaussagen welche mündliche oder auf andere Weise abgegebene Erklärungen bestätigen sollen, sondern auch für Fotokopien, Faxkopien, gescannte Dokumente und EDV-Datenträger und dessen ausgedruckten Datenbestand wie Mikrofilmreproduktionen etc. Dabei wird schriftlichen Erklärungen auf Papier (Urkunden), die dem Gericht zu Beweiszwecken vorgelegt werden, ein besonderer Beweiswert beigemessen.

2.1. Probative force of electronic documents

In a court case, probative value is crucially important. A judge is generally free to evaluate evidence and may decide, in his or her own discretion, whether a piece of evidence is credible or not, provided such evaluation is founded on verifiable arguments. This applies not only to witness statements intended to confirm evidence given verbally or by other means, but also to photocopies, fax copies, scanned documents and electronic data carriers and their printed data contents such as microfilm reproductions, etc. A special probative value is attached to written statements on paper (documents), which are laid before the court as evidence.

Elektronischen Dokumenten kommt dieser besondere Beweiswert gemäß § 371 a ZPO nur zu, soweit sie mit einer qualifizierten, elektronischen **Signatur** versehen sind. Der Sicherheitsmechanismus elektronischer Signaturen knüpft unmittelbar beim Dokument an. Ergibt die Prüfung der Signatur des elektronischen Dokumentes nach dem Signaturgesetz, dass das Dokument vom Signaturschlüssel-lnhaber signiert wurde, so wird die Echtheit der Erklärung „vermutet". Soweit kein Gegenbeweis geführt werden kann, muss sich der Signierende die Erklärung als seine eigene zurechnen lassen. Selbstverständlich können auch (nach wie vor) Papierausdrucke elektronischer Dokumente im Zivilprozess vorgelegt werden, jedoch unterliegen die dann„nur" der freien Beweiswürdigung durch den Richter.

This special probative value only attaches to electronic documents under § 371a Code of Civil Procedure (Zivilprozessordnung - ZPO) if they are stamped with a qualified electronic **signature**. The security mechanism of electronic signatures is directly tied to the document. If the verification of the signature on the electronic document according to the Digital Signature Act (Signaturgesetz) establishes that the document was signed by the signature key-owner, the authenticity of the statement is "assumed". If no evidence to the contrary can be provided, the statement must be deemed to be the signatory's own. Of course, paper printouts of electronic documents can also (as before) be submitted in civil proceedings. However, they are then subject "only" to the free assessment of evidence by the judge.

Im Ergebnis kann durch eine elektronische Signatur die Beweiskraft erhöht und über eine Beweiserleichterung rechtliche Risiken minimiert werden.

In consequence, an electronic signature can increase the probative force and by shifting the burden of proof minimize legal risks.

Die dargestellten Einschränkungen der freien richterlichen Beweiswürdigung für Urkunden im Zivilprozess gibt es im Strafprozess nicht. Der Tatrichter darf und muss jedes Beweismittel und seinen Wert selbst frei würdigen. Dabei muss der Strafrichter den Grundsatz „Im Zweifel für den Angeklagten" berücksichtigen, so dass Zweifelsfragen stets zu Lasten des Staates gehen. Zudem ist die Person, gegen die (oder deren Organisation) ermittelt wird, nicht zur Mitwirkung verpflichtet. Denn es gilt, dass niemand an der eigenen Strafverfolgung aktiv mitzuwirken verpflichtet ist.

The above limitations on a court's free assessment of documentary evidence in a civil case do not exist in German criminal proceedings. The judge himself may, and must, freely evaluate each piece of evidence and its probative value. The trial judge must give the defendant the benefit of the doubt so that the decision always goes against the state in cases of doubt. Furthermore, the accused is not obliged to cooperate or contribute anything to the criminal proceedings.

In § 98 VwGO wird für den Verwaltungsprozess auf die Regelungen des Zivilprozesses verwiesen, die im Verwaltungsprozess entsprechend anwendbar sind.

For proceedings before an administrative court, § 98 VwGO (Rules of the Administrative Courts) refers to the rules of civil proceedings, which are applicable, mutatis mutandis, in administrative proceedings.

2.2. Besonderheiten E-Mail

E-Mails werden grundsätzlich genauso behandelt wie die sonstigen elektronischen Dokumente. Im Hinblick auf deren Beweiskraft muss man wie beschrieben zwischen E-Mails mit und ohne qualifizierter elektronischer Signatur unterscheiden.

Bislang wurden in Rechtsstreitigkeiten zumeist Ausdrucke (unsignierter) E-Mails als Dokumentation elektronischer Kommunikation vorgelegt. Auch wenn es sich hierbei nicht um (unterzeichnete) schriftliche Urkunden oder ihnen gleichgestellte elektronische Dokumente mit entsprechendem Beweiswert im Sinne des Zivilprozessrechts handelt, ist ein Richter an Existenz, Inhalt und die Person des Erklärenden bereits dann gebunden, wenn der Gegner nicht bestreitet, eine Erklärung dieses Inhalts per E-Mail abgegeben zu haben. Die qualifizierte elektronische Signatur als solche (mit Verschlüsselungsvorgaben zur Gewährleistung der Integritätsprüfung) wird im konkreten Prozess insbesondere dann besondere Bedeutung erlangen, wenn die Integrität, Existenz oder die Zurechnung zum Verfasser bestritten wird.

2.2. Special characteristics of e-mails

In principle, e-mails are treated in the same way as other electronic documents. With regard to their probative force, one must distinguish, as described above, between e-mails with and without a qualified electronic signature.

In the past, printouts of (unsigned) e-mails have usually been submitted as documentation of electronic communications in litigation. Even if these do not carry the same probative value as (signed) written documents or electronic documents treated as such within the meaning of the law of civil procedure, a judge is already bound to the existence, content and person of the witness if the opponent does not dispute having sent a statement of this content by e-mail. The qualified electronic signature (with specifications for encryption to ensure the integrity check) as such will then assume particular significance in the actual case especially if the integrity, existence or attribution to the author is disputed.

2.3. Beweislast des Zuganges

Erklärt eine Partei im Prozess, eine E-Mail nie erhalten zu haben, so handelt es sich um ein Zugangsproblem, das bei postalischer Briefbeförderung schon lange bekannt ist: die Beweislast für den Zugang trifft in diesem Fall den Absender. Hier könnte eine qualifizierte elektronische Signatur nur dann Abhilfe schaffen, wenn der Empfänger automatisiert eine qualifiziert elektronisch signierte Rückmail (Antwortmail unter Beifügung des ursprünglichen Textes) absetzt, was juristisch eine sog. „Empfangsbekenntnis“ darstellt oder sich eines "elektronischen Einschreibens" bedient.

Erklärt eine Partei im Prozess, eine E-Mail nie versendet zu haben, so wird sie zur Plausibilisierung vortragen müssen, wie der Empfänger dennoch zu dieser Mail gekommen ist. Hier sind im wesentlichen zwei Fälle denkbar: zum einen kann der Zugang unerlaubt benutzt worden sein (Ausspähen des Passworts durch einen Dritten etc.), zum anderen kann sich der Empfänger die E-Mail „ausgedacht“ haben (Totalfälschung). An dieser Stelle kann eine qualifizierte elektronische Signatur die Rechtsposition deutlich stärken. Für Dokumente, für welche keine gesetzlichen Aufbewahrungspflichten bestehen, ist unabhängig davon stets zu entscheiden, ob diese dennoch im eigenbetrieblichen Interesse elektronisch aufbewahrt werden sollten.

2.3. Burden of proof of receipt

If a litigating party in the case denies ever having received an e-mail, this is a problem of receipt, which has long been an issue in the handling of postal correspondence: in such a case the burden of proof of receipt is on the sender. A qualified electronic signature could only be of assistance in this case if the recipient sends an automated return mail with a qualified electronic signature (reply mail which includes the original text), which legally constitutes a so-called “acknowledgement of receipt”, or uses “electronic registered post”.

If, during the proceedings, a party denies ever having sent an e-mail, the party is obliged to explain how the recipient has nevertheless received the e-mail. There are basically two possible cases: one is that the internet access was used without authorization (password spied out by a third party, etc.);the other is that the recipient has “made up” the e-mail (total forgery). In such a case, a qualified electronic signature can significantly strengthen the legal position. With regard to documents not subject to any legal retention obligations one must always decide whether they should nevertheless be stored electronically in the company’s own interests.

2.4. Haftung vermeiden

Die Verletzung von Aufbewahrungspflichten kann straf- und berufsrechtliche, aber auch prozessuale Konsequenzen haben. Beispiele: Die Verletzung der handelsrechtlichen Buchführungspflicht kann eine Straftat nach § 283 b, § 274 StGB bzw. nach § 370 AO sowie eine Ordnungswidrigkeit wegen Steuergefährdung nach § 379 AO darstellen. Geschäftsführer oder Vorstände der betroffenen Gesellschaften kann bei der Verletzung von Aufbewahrungspflichten eine Schadensersatzpflicht nach § 43 Abs. 2 GmbHG bzw. § 92 Abs. 2 AktG treffen.

2.4. Avoiding liability

A breach of retention obligations could have penal, professional and procedural, consequences. Examples: A breach of the mandatory duty to keep books of account under commercial law may be an offence under § 283b, § 274 German Penal Code (Strafgesetzbuch – StGB) or under § 370 AO. It may also constitute an administrative offence for minor tax fraud under § 379 AO. A breach of retention obligations may result in the CEOs or directors of the affected companies becoming liable for damages under § 43 Paragraph 2 German Limited Liability Companies Act (Gesetz betreffend die Gesellschaften mit beschränkter Haftung - GmbHG) or § 92 Paragraph 2 German Companies Act (Aktiengesetz - AktG).

Im Rahmen der prozessualen Konsequenzen ist § 427 ZPO zu beachten. Danach gilt der Inhalt der Abschrift einer Urkunde als bewiesen, wenn der Gegner der Anordnung, die in seinen Händen befindliche Urkunde vorzulegen, nicht nachgekommen ist.

3. Elektronische Aufbewahrung von kaufmännischen Unterlagen im Ausland

Zunächst gilt der Grundsatz, dass Bücher und sonst erforderlichen Aufzeichnungen im Geltungsbereich der Abgabenordnung zu führen und aufzubewahren sind. Auf Grundlage von § 146 Absatz 2a AO (in der Fassung des Jahressteuergesetzes 2010) dürfen Unternehmen ihre elektronischen Bücher und sonstigen erforderlichen elektronischen Aufzeichnungen oder Teile davon im Ausland führen und aufbewahren. Hierfür bedarf es allerdings der Bewilligung der Finanzverwaltung, die vom Vorliegen bestimmter Voraussetzungen abhängt.

Voraussetzungen sind, dass:

1. der Steuerpflichtige der zuständigen Finanzbehörde den Standort des Datenverarbeitungssystems und bei Beauftragung eines Dritten dessen Namen und Anschrift mitteilt.
2. der Steuerpflichtige seinen steuerlichen Mitwirkungspflichten ordnungsgemäß nachgekommen ist.
3. der Datenzugriff nach § 147 Abs. 6 AO in vollem Umfang möglich ist.
4. die Besteuerung nicht beeinträchtigt ist.

Soweit dem Antrag statt gegeben wird, ist die Verlagerung nicht nur in Staaten der EU / EWR beschränkt, sondern auch in andere Staaten möglich. Die Entscheidung über die Bewilligung steht im Ermessen der Behörde.

Die deutsche Fassung geht vor. Die englische Fassung dient allein der Information.

With regard to procedural consequences, § 427 ZPO should be noted. This provides that the content of the copy of a document is deemed to be proved if the opposing party fails to submit the document in his possession.

3. Electronic Storage of Financial Documents Abroad

The principle at issue relates to the regulations governing the maintenance and storage of accounts and other essential records under German tax law. Under the terms of § 146 2a AO (German Tax Code for 2010 tax year), companies are allowed to maintain and store their electronic accounts and other essential electronic records or parts thereof outside Germany. However, they do require permission from the tax authorities in order to do so, and this permission depends on the fulfillment of certain conditions.

These conditions are:

1. The party liable for tax must inform the responsible tax authority of the location of the data processing system and, in the case of outsourcing, the name and address of the third party responsible for the system.
2. The party liable for tax has fulfilled all of his or her tax obligations correctly.
3. Access to the data is complete and unrestricted pursuant to § 147 section 6 AO (German Tax Code).
4. The tax assessment is not affected.

If the application is granted, the relocation is not restricted only to the states of the EU/EEA, but covers other states as well. The decision on approval is made at the discretion of the authority.

The German version shall prevail. The English version is for information purposes only.

Disclaimer

Die dargestellten Ausführungen sind ohne Gewähr und sollen Ihnen die Probleme in groben Zügen überblicksweise und ohne Anspruch auf Vollständigkeit und Detailgenauigkeit näher bringen. Die vorliegenden Ausführungen sind nicht geeignet, Einzelheiten der jeweiligen gesetzlichen Regelungen und alle Aspekte der angesprochenen Themen zu beleuchten und ersetzt nicht die rechtliche und steuerliche Beratung im Einzelfall. Vor geschäftlichen Entscheidungen setzen Sie sich bitte mit Ihrem Steuerberater, Wirtschaftsprüfer oder Rechtsanwalt in Verbindung. Die gesetzlichen Regelungen können sich seit Erscheinen dieses Textes geändert haben.

Disclaimer

The information provided above is without engagement and is intended solely to provide you with a general overview of the problems without any pretension to completeness or accuracy of detail. This Statement is not designed to clarify the details of individual legal regulations or all aspects of the subjects addressed and does not replace legal and tax advice in individual cases. Before making any business decisions you should consult your tax adviser, auditor or attorney. The legal regulations may have changed since this text was published.

Italy

Author:

Andrea Lisi

Avvocato residente a Lecce, è specializzato in Diritto Europeo ed esperto di problematiche internazionali, incluse quelle associate a nuove tecnologie, fatturazione elettronica e tutela della privacy.

È inoltre presidente dell'Associazione nazionale per operatori e responsabili della conservazione digitale (A.N.O.R.C.), prima associazione di questo tipo in Italia.

E-mail: andrealisi@scintlex.it

Andrea Lisi

Lawyer in Lecce, specialized in EU Law and expert in international issues, also those related to new technologies, e-invoicing and privacy safeguard.

He is also Chairman of the first Italian Association of Person Liable for Electronic & Fiscal Archive, called A.N.O.R.C.

e-mail: andrealisi@scintlex.it

1. Premesse generali sulla legislazione italiana in materia di digitalizzazione documentale

In Italia esiste una copiosa e complessa normativa in materia di formazione, spedizione, protocollazione, archiviazione, fascicolazione, conservazione, esibizione dei documenti informatici giuridicamente rilevanti.

L'iter legislativo in materia si è avviato nei primi anni '90 per giungere in quest'ultimo periodo ad una maturità che consente ormai una completa gestione "paperless" dell'azienda o della pubblica amministrazione.

La stessa normativa rende possibile in molti casi la sostituzione dell'archivio cartaceo attraverso un processo di scansione del documento rilevante giuridicamente e la sua conservazione a norma in un archivio digitale, attraverso la predisposizione di un sistema di conservazione cosiddetta sostitutiva.

Qui di seguito riportiamo la principale normativa italiana attualmente in vigore in materia di digitalizzazione documentale suddivisa per macroaree:

1.1. NORMATIVA GENERALE

- **Decreto Legislativo 7 marzo 2005, n. 82:** Codice dell'Amministrazione Digitale (come modificato dal D. Lgs. 159/2006), di seguito anche CAD

1. General Background on Italian legislation on the digitization of documents

In Italy there are copious and complex regulations regarding the creation, dispatch, registration, storage, collation, preservation and presentation of legally relevant electronic documents.

The legislative process in this area began in the early 1990s and has now reached a level of maturity that allows completely paperless management of a company or public administration.

In many cases, the same regulations make possible the replacement of the paper archive by scanning the legally relevant document and storing it in a digital archive in accordance with the law, by implementing what is known as a replacement storage system.

The main Italian legislation currently in force with regard to the digitization of documents is sub-divided into high-level areas:

1.1. GENERAL RULES

- **Legislative Decree 7 March 2005 No 82:** Digital Administration Code (as amended by Legislative Decree no. 159/2006), hereafter also referred to as CAD

- **Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009** - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici, di seguito anche DPCM 30 marzo 2009

1.2. NORMATIVA SULLA POSTA ELETTRONICA CERTIFICATA

- **Decreto del Presidente della Repubblica 11 Febbraio 2005, n. 68** - Disposizioni per l'utilizzo della Posta Elettronica Certificata, di seguito anche DPR sulla PEC
- **Decreto Ministeriale 2 novembre 2005** - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata"
- Articoli 16 e 16 bis della **Legge 28 gennaio 2009, n. 2** - Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale (contiene norme specifiche sull'obbligatorietà della PEC per determinati soggetti giuridici)
- **Decreto del Presidente del Consiglio dei Ministri 6 maggio 2009** - Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini

1.3. NORMATIVA IN MATERIA TRIBUTARIA

- **Decreto Legge 10 giugno 1994, n.357**, convertito dalla legge 8 agosto 1994 n.489, contenente Disposizioni tributarie urgenti per accelerare la ripresa dell'economia e dell'occupazione, nonché per ridurre gli adempimenti a carico del contribuente

- **Decree of the President of the Council of Ministers dated 30 March 2009** - Technical rules relating to the generation, attachment and verification of digital signatures and time validity of electronic documents, hereafter also referred to as the 30 March 2009 DPCM

1.2. LEGISLATION ON CERTIFIED MAIL

- **Decree of the President of the Republic dated 11 February 2005 No. 68** – Provisions for the use of Certified Electronic Mail, hereafter also referred to as DPR on CEM
- **Ministerial Decree dated 2 November 2005** - Technical rules for the creation, transmission and validation, including time validation, of Certified Electronic Mail
- Articles 16 and 16a of Law **No. 2 dated 28 January 2009** - Conversion into law, with amendments, of Decree Law No. 185 dated 29 November 2008 on emergency measures to support families, jobs, employment and business and for the redesign, for crisis response, of the National Strategic Framework (contains specific rules on obligatory nature of CEM for certain legal entities)
- **Decree of the President of the Council of Ministers dated 6 May 2009** - Provisions regarding the issue and use of certified electronic mailboxes assigned to citizens

1.3. TAX LEGISLATION

- **Decree Law No. 357 dated 10 June 1994**, converted into law No. 489 on 8 August 1994, containing emergency tax provisions to accelerate recovery of the economy and employment and to reduce the burden to the taxpayer

- **Decreto 23 gennaio 2004 del Ministero dell'Economia e delle Finanze** inerente alle modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporti, di seguito anche DMEF 23 gennaio 2004
- **Decreto Legislativo. 20 febbraio 2004, n. 52** riguardante l'attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA, di seguito anche D. Lgs. 52/2004
- **Circolare 6 dicembre 2006, n. 36 dell'Agenzia delle Entrate** - Decreto ministeriale 23 gennaio 2004 – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto
- **Circolare 19 ottobre 2005, n. 45 dell'Agenzia delle Entrate** - Decreto legislativo 20 febbraio 2004, n. 52 - Attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA

- **January 23 2004 Decree of the Ministry of Economy and Finance** on arrangements for the fulfillment of tax obligations relating to electronic documents and their reproduction in different types of media, hereafter also referred to as January 23 2004 DMEF
- **Legislative Decree No. 52 dated 20 February 2004** regarding implementation of directive 2001/115/CE simplifying and harmonizing VAT billing methods, hereinafter also Legislative Decree 52/2004
- **Revenue Agency Memorandum No. 36 dated 6 December 2006** - Ministerial Decree dated 23 January 2004 - Arrangements for the fulfillment of tax obligations relating to electronic documents and their reproduction in different types of media
- **Revenue Agency Memorandum No. 45 dated 19 October 2005** - Legislative Decree No. 52 dated 20 February 2004 - Implementation of Directive 2001/115/EC, which simplifies and harmonizes arrangements for VAT billing

1.4. NORMATIVA IN MATERIA DI DOCUMENTI DEL LAVORO

- articoli 39 e 40 della **Legge 6 agosto 2008, n. 133** - Conversione in legge, con modificazioni, del decreto-legge 25 giugno 2008, n. 112, recante disposizioni urgenti per lo sviluppo economico, la semplifi-cazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione tributaria (contiene le norme generali sulla tenuta informatica del Libro Unico del Lavoro)
- **Decreto Ministero Lavoro 9 luglio 2008** - Istituzione e tenuta del Libro unico del lavoro
- **Circolare n. 20/2008 del 21 agosto 2008 Ministero Lavoro** (contiene le istruzioni operative per il personale ispettivo)

1.4. RULES ON EMPLOYMENT DOCUMENTS

- Articles 39 and 40 of Law **No. 133 dated 6 August 2008** - Conversion into law, with amendments, of Decree Law No. 112 dated 25 June 2008, on emergency measures for economic development, simplification, competitiveness and stabilization of public finances and tax equalization (contains the general rules on computer processing for the Single Employment Ledger)
- **Decree of the Ministry of Labor dated 9 July 2008** - Set-up and processing of the Single Employment Ledger
- **Ministry of Labor Memorandum No. 20/2008 21 August 2008**, (includes operating instructions for inspection staff)

1.5. NORMATIVA IN MATERIA DI REGISTRI E CONTRATTI ASSICURATIVI

- **Regolamento ISVAP n. 27 del 14 ottobre 2008** concernente la tenuta dei registri assicurativi di cui all'articolo 101 del decreto legislativo 7 settembre 2005, n. 209 – codice delle assicurazioni private

1.6. RIFERIMENTI TECNICI

- **Deliberazione CNIPA 19 febbraio 2004 n. 11** - Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali, di seguito anche Deliberazione CNIPA n. 11/2004
- **Deliberazione CNIPA 21 maggio 2009, n. 45** - contenente le Regole per il riconoscimento e la verifica del documento informatico

1.5. RULES ON INSURANCE CONTRACTS AND RECORDS

- **ISVAP Regulation No. 27 dated 14 October 2008** concerning the retention of insurance records covered by Article 101 of Legislative Decree No. 209 dated 7 September 2005 - Code of Private Insurance

1.6. TECHNICAL REFERENCES

- **CNIPA Resolution No. 11 dated 19 February 2004** - Technical Rules for the reproduction and storage of documents on optical media such as to ensure conformity with the originals, hereinafter also referred to as CNIPA Resolution No. 11/2004
- **CNIPA Resolution No. 45 dated 21 May 2009** – containing rules for recognition and verification of electronic documents

2. Valore formale e probatorio del documento informatico

Nel Codice dell'Amministrazione Digitale (Decreto Legislativo 7 marzo 2005, n. 82, di seguito CAD), testo normativo fondamentale in materia di digitalizzazione documentale per PA e privati, vengono definiti i concetti di **documento informatico** (quale "rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti"), di **firma elettronica** (e, cioè, "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica") e firma digitale (definita come "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici").

2. Formal and probative value of electronic documents

The Digital Administration Code (Legislative Decree No. 82 dated 7 March 2005, hereinafter referred to as CAD), the basic legal text in the digitization of documents for PA (Public Administration) and private agencies, defines the concepts of **electronic document** (as "computer representation of legally-relevant acts, facts and data"), of electronic signature ("all data in electronic form logically attached to or associated with other electronic data, used as a method of electronic identification") and **digital signature** (defined as "a special type of qualified electronic signature based on a system of linked cryptographic keys, one public and one private, which allows the owner through the private key and the recipient through the public key, respectively, to display and verify the origin and integrity of an electronic document or a set of electronic documents").

I **documenti informatici privi di firma elettronica** vengono ricondotti per i loro effetti giuridici alle riproduzioni fotografiche o cinematografiche, alle registrazioni fonografiche e, in genere, ad ogni altra rappresentazione meccanica o informatica di fatti o cose, la cui efficacia probatoria è disciplinata dall'articolo 2712 codice civile (così si è pronunciata la Suprema Corte di Cassazione sez. civile 6.12.2001, n. 11445). In caso di disconoscimento, concernendo fatti e non regole, questo non preclude al giudice di utilizzare liberamente il documento, apprezzandone l'attendibilità, per formare il proprio convincimento.

Electronic documents without an electronic signature refer, for legal purposes, to photographic reproductions or film, sound recordings and, generally, to any other mechanical or computer representation of facts or things, whose probative value is governed by Article 2712 of the Civil Code (as ruled in the Supreme Court of Cassation civil section, 6.12.2001, No. 11445). Repudiation of facts, as opposed to rules, does not preclude the court from freely using the document, when it is judged to be reliable, to arrive at its own opinion.

Il **documento con firma elettronica** "semplice" può soddisfare il requisito della "forma scritta" ed è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza, integrità e immodificabilità.

A document with a "simple" **electronic signature** may meet the requirement of "written form" and may be freely assessed in court, taking into account its objective characteristics of quality and security, integrity and non-modifiability.

Il **documento informatico a cui è apposta una firma digitale** o altro tipo di firma elettronica qualificata soddisfa sempre il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12, del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria.

An **electronic document to which a digital signature** or other qualified electronic signature is attached satisfies the requirement of "written form", even in cases provided for under penalty of invalidity, of Article 1350, first paragraph, Nos. 1 through 12 of the Civil Code. The use of the signature device is presumed to be attributable to the owner, unless they can prove otherwise.

Per i documenti informatici il CAD definisce un importante strumento, quello della **validazione temporale**, definendola come il "risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi". Tale validazione temporale assume nei riguardi del documento informatico la funzione di disciplinare le modalità di computazione della data rispetto ai terzi, in modo analogo a quanto previsto per il documento cartaceo: con la validazione viene apposto sul documento informatico un "segno" digitale che ha lo scopo di rendere certa ed opponibile ai terzi la data (e l'ora) di formazione del documento.

For electronic documents the CAD defines an important tool, **time validation**, defined as the "result of the computer procedure which is used to attach a date and a time enforceable against third parties to one or more electronic documents". This time validation takes on, for electronic documents, the regulation of the means of computation of the date with respect to third parties, in a similar way to the provisions for paper documents: validation involves attachment to the electronic document of a digital "sign" that has the purpose of making certain and enforceable against third parties the date (and time) of the creation of the document.

3. Posta elettronica semplice e Posta Elettronica Certificata

In Italia, nell'ambito del diritto civile e amministrativo, non esiste una regolamentazione normativa specifica in materia di comunicazioni e-mail, le quali possono comunque assumere valore in giudizio quali documenti informatici con firma elettronica semplice e, inoltre, molti Tribunali hanno ritenuto il messaggio e-mail (anche privo di firma digitale) quale **valida prova scritta per l'ottenimento di un decreto ingiuntivo**. Ovvio che la trasmissione di semplici e-mail, seppure sia un sistema molto utilizzato, si presta a possibili contestazioni in giudizio e non è dotata di garanzie certe sul mittente che ha spedito il messaggio, sull'orario di invio, sulla notifica di ricezione e su altri elementi del messaggio di posta elettronica. Per questo si è avvertita la necessità di dotarsi di un sistema di comunicazione che dia maggiori garanzie, senza perdere i vantaggi dell'e-mail tradizionale. È nata così in Italia la Posta Elettronica Certificata (c.d. **PEC**) che consiste in un sistema di posta elettronica nel quale, a seguito dell'invio del messaggio/documento informatico viene fornita al mittente una documentazione elettronica, con valenza legale, attestante l'invio e la consegna dei messaggi/documenti informatici. Tale strumento, paragonabile a una vera e propria lettera raccomandata con ricevuta di ritorno, è oggi obbligatorio per determinate categorie professionali, per le società e per le pubbliche amministrazioni.

Possono scambiarsi e-mail certificate sia i privati, sia le pubbliche amministrazioni. Sono i **gestori del servizio PEC**, iscritti in apposito elenco tenuto dall'ente DigitPA (che verifica i requisiti soggettivi ed oggettivi inerenti, ad esempio, alla capacità ed esperienza tecnico-organizzativa, alla dimestichezza con procedure e metodi per la gestione della sicurezza, alla certificazione ISO9000 del processo), a fare da garanti dell'avvenuta consegna. Il sistema deve garantire che i messaggi di PEC vengano sottoscritti con la firma elettronica avanzata che deve essere apposta sia sulla busta, sia sulle ricevute rilasciate dai gestori per assicurare l'integrità e l'autenticità del messaggio.

3. Simple and certified electronic mail

In Italy's civil and administrative law, there is no specific legislation relating to e-mail communications, which may however have legal value as electronic documents with a simple electronic signature and, moreover, many courts have considered e-mail (even without digital signature) **valid written proof for obtaining an injunction**. Obviously, the transmission of simple e-mails, even if it is a widely used system, lends itself to possible challenges in court and offers no certain guarantees as to the person who sent the message, the time it was sent, or notification of receipt and other elements of the e-mail message. For this reason the need was highlighted to provide a communication system that offers greater guarantees, but without losing the advantages of traditional e-mail. Certified Electronic Mail (**CEM**) was thus born in Italy. CEM consists of an electronic mail system in which, after sending the message / electronic document the sender is provided with legally valid electronic documentation attesting to the dispatch and delivery of electronic messages / documents. This tool, similar to a real letter registered with a return receipt, is now mandatory for certain professional categories, for companies and for the public administration.

Private parties and public administrations may exchange certified e-mails. It is the **operators of the CEM service**, registered in a special list kept by the organization DigitPA (which checks the subjective and objective requirements regarding, for instance, technical /organizational capacity and experience, familiarity with procedures and methods for security management, ISO9000 certification of the process), to guarantee delivery. The system must guarantee that CEM messages are signed with an advanced electronic signature, which must be applied both to the envelope and to the receipts issued by the operators to guarantee the integrity and authenticity of the message.

Ai sensi **dell'art. 45 del CAD** "i documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore".

La comunicazione telematica viene tutelata nella sua riservatezza, anche dal punto di vista penale. In particolare, **l'art. 616 codice penale** rubricato "violazione, sottrazione e soppressione di corrispondenza" opera una piena equiparazione tra corrispondenza cartacea e telematica affermando che "agli effetti delle disposizioni di questa sezione, per corrispondenza si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza". Inoltre, secondo **l'art. 49 del CAD** "gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario".

According to **Art. 45 of CAD**, "documents submitted by anyone to the public administration by any electronic means, including fax, such as to make possible verification of the original source, satisfy the requirement of "written form" and the transmission need not be accompanied by that of the original document.

2. Electronic documents transmitted electronically are considered sent by the sender to his/her provider, and are understood to be delivered to the addressee if made available at addressee's electronic address, in the addressee's email inbox made available by the provider."

The confidentiality of electronic communication is protected, also from the standpoint of criminal law. In particular **Art. 616 of the Penal Code** entitled "breach, misappropriation and removal of correspondence" treats paper and electronic mail as fully equivalent, stating that "for the purposes of the provisions of this section, correspondence means letters, telegraphic and telephonic communication, computer or other electronic communication or correspondence made with other forms of distance communication". Furthermore, according to **Art. 49 of the CAD**, "Persons using electronic transmission of formatted records, data and documents using computer technology may not take cognizance of the electronic correspondence, copy it by any means or pass on the information to third parties in any capacity, even as a summary or as an extract of the existence or content of the correspondence, communications or messages transmitted by electronic means, except in the case of information which, by its nature or by express indication of the sender, is intended for the public domain. For purposes of this Code, records, data and documents transmitted electronically are considered, in the context of the operator of the information transmission system, the property of the sender until they have been delivered to the recipient."

4. Fattura inoltrata telematicamente e Fattura Elettronica

Già con la Risoluzione del 30/07/1990 prot. 450217 il Ministero dell'Economia e delle Finanze ha riconosciuto la **legittimità dei dati trasmessi per via telematica**, fermo restando il rispetto della regolamentazione di operazioni rilevanti ai fini dell'Iva, ovvero i dati contenuti nel documento conservato dall'emittente e in quello inviato al cliente devono essere i medesimi. Questa posizione ministeriale, ribadita in diverse risoluzioni successive, è stata confermata nella Circolare n. 45/E del 19 ottobre 2005 dell'Agenzia delle Entrate, secondo la quale "anche la fattura in formato cartaceo può essere creata attraverso uno strumento informatico; tuttavia, a differenza della fattura elettronica, le parti dell'operazione hanno l'obbligo di materializzare il documento informatico su un supporto cartaceo, che costituisce, in questo caso, l'originale della fattura. In tale evenienza, la materializzazione si rende necessaria in quanto il documento è carente dei requisiti (riferimento temporale e firma elettronica qualificata) che caratterizzano la fattura elettronica, garantendone la data certa e l'immodificabilità del contenuto". Quindi, **per evitare la stampa delle fatture trasmesse via e-mail occorre rispettare i requisiti previsti nel D. Lgs. 52/2004**: in questo caso, la fattura deve essere emessa elettronicamente e, cioè, la fattura deve nascere, deve essere trasmessa e conservata esclusivamente in formato digitale sia dall'emittente sia dal destinatario (nel momento in cui vi è un accordo sulla trasmissione elettronica della stessa). **La fattura elettronica viene definita dalla Circolare 45/2005 dell'Agenzia delle Entrate** come il "documento informatico, predisposto in forma elettronica, secondo specifiche modalità che garantiscono l'integrità dei dati contenuti e l'attribuzione univoca del documento al soggetto emittente, senza necessità di provvedere alla stampa su supporto cartaceo".

La fattura elettronica, in particolare, non deve contenere macroistruzioni né codici eseguibili, e l'attestazione della data, l'autenticità dell'origine e l'integrità del contenuto della fattura stessa sono garantite rispettivamente mediante l'apposizione, su ciascuna fattura o su un lotto di fatture, del riferimento temporale

4. Electronic bill delivery and electronic bills

In Resolution dated 30/07/1990, Prot. 450217, the Economy and Finance Ministry had already recognized the **legitimacy of electronically transmitted data**, subject to compliance with the regulations of the relevant transactions for VAT purposes, i.e. the data contained in the documents kept by the issuer and the data in the document sent to the customer must be identical. This ministerial position, repeated in a number of subsequent resolutions, was confirmed in Revenue Agency Memorandum No. 45/E dated 19 October 2005, under which "invoices in printed form may also be created using a computerized tool; however, unlike electronic invoices, the parties to the transaction are required to give the computerized document material form on paper, which in this case constitutes the original invoice. In this case, material form is necessary as the document does not meet the requirements (time reference and qualified electronic signature) characterizing the electronic invoice, guaranteeing certainty of the date and non-modifiability of the content". Therefore, **in order to avoid the printing of invoices sent by e-mail, the requirements of Decree Law 52/2004** must be met: in this case, the invoice must be issued electronically, i.e., the invoice shall be created, must be transmitted and stored exclusively in digital format either by the issuer or by the recipient (when there is an agreement on the electronic transmission of the invoice). **The electronic invoice is defined by Revenue Office Memorandum 45/2005** as the "computer document, prepared in electronic form in accordance with specific arrangements to guarantee the integrity of the data contained and the unambiguous attribution of the document to the issuing person, without the need to arrange for printing on paper".

The electronic invoice, in particular, should not contain executable code or macros, and certification of the date, the authenticity of the origin and integrity of the contents of the bill itself are guaranteed respectively by attaching to each invoice, or batch of invoices, the time reference (understood as internal time

(inteso come validazione temporale interna) e della firma elettronica qualificata dell'emittente, o mediante sistemi EDI di trasmissione elettronica dei dati che garantiscano i predetti requisiti di autenticità ed integrità.

Si ricorda, infine, che Il D. Lgs. 52/2004 ha apportato modifiche agli articoli 39 e 52 del decreto del Presidente della Repubblica n. 633 del 1972 concernenti rispettivamente "la tenuta e conservazione dei registri e dei documenti" e gli "accessi, ispezioni e verifiche". In particolare, si annuncia la possibilità di un accesso telematico all'archivio fiscale, ma l'intervento più rilevante consiste nell'aver previsto la possibilità di conservare le fatture in forma elettronica in un Paese estero con il quale esistono strumenti giuridici che disciplinano la reciproca assistenza.

5. La conservazione sostitutiva dei documenti

La conservazione sostitutiva può essere definita come quel procedimento che permette di assicurare la validità legale nel tempo a un documento *ab origine* informatico o a un documento analogico successivamente digitalizzato.

Questa tipologia di processi consente di conferire la stessa efficacia giuridica dei documenti cartacei a quelli elettronici e permette alle aziende e all'amministrazione pubblica di risparmiare sui costi di stampa, di stoccaggio e di archiviazione cartacea o comunque di liberare archivi cartacei rimpiazzandoli con sistemi di conservazione sostitutiva.

Ai fini di una corretta conservazione occorre realizzare un processo che permetta di assecondare gli attuali parametri tecnici fissati dal CNIPA (contenuti nella Deliberazione 11/2004 per la conservazione dei documenti) e, per quanto concerne i documenti rilevanti ai fini tributari, dal Decreto del Ministero dell'Economia e delle Finanze del 23 Gennaio 2004.

validation) and the qualified electronic signature of the issuer or through EDI systems for electronic transmission of data to ensure the above-mentioned requirements of authenticity and integrity.

Lastly, note that Legislative Decree 52/2004 introduced amendments to articles 39 and 52 of the President of the Republic's Decree No. 633 of 1972 respectively concerning "the keeping and conservation of registers and documents" and "access, inspection and verification". In particular, the possibility of computerized access to the fiscal archives is envisaged, but the most important change consists of envisaging the possibility of keeping invoices in electronic form in a foreign country with which there are legal tools governing reciprocal assistance.

5. Electronic document storage

Electronic storage can be defined as those processes that enable assurance of the legal validity in time of a document which is electronic *ab origine* or a similar document that is later digitized.

This type of process enables the same legal status conferred on paper documents to be applied to electronic ones and enables companies and the public administration to save on printing costs, storage and paper-based archiving or otherwise dispense with paper files, by replacing them with systems of electronic storage.

For the purposes of correct storage it is necessary to implement a process that conforms to the current technical parameters set by CNIPA (contained in Resolution 11/2004 for document retention) and, as regards documents relevant for tax purposes, the Decree of the Ministry of Economy and Finance dated 23 January, 2004.

In particolare, secondo **l'art. 44 del CAD**, "il sistema di conservazione dei documenti informatici deve garantire:

- l'identificazione certa del soggetto che ha formato il documento;
- l'integrità del documento;
- la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;
- il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto".

5.1. il processo di conservazione dei documenti originariamente informatici

Il processo avviene mediante memorizzazione su supporti ottici (o comunque supporti informatici idonei) e si conclude con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, della firma digitale e della marca temporale (quale validazione temporale opponibile a terzi) ad opera del Responsabile della conservazione che certifica, in tal modo, l'esatto svolgimento del processo.

La normativa precisa, quindi, che la firma digitale del Responsabile può essere apposta sul lotto di documenti da conservare o su un'evidenza informatica che contiene l'insieme delle impronte degli stessi. La normativa italiana prevede anche, all'art. 35 comma 3 del CAD la possibilità di utilizzare **procedure automatiche di firma digitale** per sviluppare tali processi.

In particular, according to **Art. 44 of the CAD**, "the computer document conservation system must guarantee:

- The certain identification of the person who created the document;
- The integrity of the document;
- The readability and easy availability of documents and the identifying information, including original registration and classification data;
- Compliance with the security measures provided for in Articles 31 to 36 of Decree No. 196 of 30 June 2003, and the Technical Regulations published in Annex B of the decree."

5.1. The storage process for electronic documents (ab origine)

The process takes place via storage on optical media (or other suitable media) and ends with the attachment to all documents, or to an electronic proof containing one or more fingerprints of documents or groups of documents, of the digital signature and time stamp (as a time validation enforceable against third parties) by the person responsible for storage, which certifies the exact development of the process.

The law therefore states that the digital signature of the person responsible for storage may be applied to a batch of documents to be stored or to an electronic proof containing the set of fingerprints of the documents. Italian law also envisages, in art. 35 no. 3 of the CAD, the possibility of using **automatic digital signature procedures** for performing these processes.

5.2. il processo di conservazione sostitutiva di documenti originariamente analogici

Il processo di conservazione sostitutiva di documenti analogici avviene mediante memorizzazione della relativa immagine direttamente sui supporti ottici (o supporti idonei), eventualmente, anche della relativa impronta, e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, della firma digitale e della marca temporale da parte del Responsabile della conservazione che attesta così il corretto svolgimento del processo.

La distruzione di documenti analogici, di cui è obbligatoria la conservazione, è consentita soltanto dopo il completamento della procedura di conservazione sostitutiva.

5.2. The storage process for electronic documents (originally analogue)

The process of electronic storage of analog documents takes place by storing their image directly on optical media (or other suitable media), and possibly also the fingerprint, and ends with the attachment to all documents or to electronic evidence containing one or more fingerprints of the documents or groups of documents, of the digital signature and time stamp by the person responsible for storage which attests the correct performance of the process.

The destruction of analog documents, whose storage is required, is only allowed after the completion of electronic storage.

5.3. il formato del documento da conservare

Il documento informatico per poter passare in conservazione deve essere statico e non modificabile e, cioè, redatto in modo tale per cui il contenuto risulti inalterabile durante le fasi di accesso e di conservazione, nonché immutabile nel tempo; a tal fine il documento informatico non deve contenere macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

5.3. The format of the document to be stored

In order to store the electronic document it must be static and non-modifiable, that is, it must have been produced in such a way that the content cannot be modified during the access and storage phases, or over time; for this purpose the electronic document should not contain executable code or macros to activate functions that could alter the records, facts or data contained in the document.

5.4. il supporto di conservazione

È possibile utilizzare supporti dotati di tecnologia laser, come i dischi ottici (Cd-R e Dvd, provvisti di notevole capacità di memorizzazione), o altri idonei supporti di memorizzazione digitale (come qualsiasi sistema di storage); l'unico limite alla libera scelta è costituito dal fatto che tali supporti devono comunque garantire la conformità dei documenti agli originali e la leggibilità del loro contenuto nel tempo.

5.4. Storage media

It is possible to use laser technology, such as optical discs (CD-R and DVD, with high storage capacity), or other suitable digital storage media (such as any storage system); the only limit to free choice is the fact that these media must still ensure conformity of the electronic documents with the originals and the readability of their contents over time.

5.5. l'esibizione avanti le autorità di vigilanza

Qualora si renda necessario un controllo o un'ispezione ad opera dell'Amministrazione, sia il documento informatico sia quello analogico, conservato su supporto informatico, devono essere resi leggibili presso il sistema di conservazione sostitutiva e, a seguito di eventuale richiesta, resi disponibili su carta.

In caso di inosservanza delle norme sulla corretta conservazione o sul corretto trattamento dei dati personali contenuti nei documenti conservati sono applicabili sanzioni amministrative (e anche sanzioni di rilevanza penale).

5.5. Exhibition to surveillance authorities

For monitoring or inspection by the administration, whether the document is electronic or an analog document stored on electronic media, it must be made legible by the system of electronic storage and, where requested, made available on paper.

In case of non-compliance with the law on the proper storage or on the proper handling of personal data contained in the stored documents, administrative sanctions are applicable (including penalties and criminal law).

5.6. i documenti conservabili digitalmente

È possibile conservare digitalmente tutti i documenti contabili (fatture, ricevute fiscali, lettere, telegrammi, documenti di trasporto, scritture, registri e libri etc.), le dichiarazioni fiscali e la modulistica relativa ai pagamenti, i documenti inerenti al rapporto di lavoro (Libro Unico del Lavoro e cedolini paga), i registri e le polizze assicurative.

5.6. Digitally storable documents

It is possible to store digitally all accounting documents (invoices, tax receipts, letters, telegrams, transport documents, writings, records and books etc.), tax returns and forms relating to payments, documents pertaining to labor relations (Single Employment Ledger and pay-slips), records and insurance policies.

5.7. la durata della conservazione

Secondo l'art. 2220 del codice civile tutte le scritture contabili devono essere conservate per dieci anni dalla data dell'ultima registrazione. Per lo stesso periodo devono conservarsi le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti.

5.7. Storage duration

According to Article 2220 of the Civil Code, all accounting records must be retained for ten years from the date of registration. Invoices must be kept for the same period, as must letters and telegrams received and copies of invoices, letters and telegrams sent.

5.8. il Responsabile della conservazione

Il processo di conservazione dei documenti informatici deve essere affidato ad una figura altamente specializzata e competente.

5.8. The person responsible for storage

The retention of electronic documents should be entrusted to a highly skilled and competent individual.

La deliberazione CNIPA del 2004 n. 11 definisce le funzioni del responsabile della conservazione sostitutiva, attribuendogli scrupolosi compiti e responsabilità. In particolare, tale figura ha l'obbligo di creare un database relativo ai documenti informatici nel rispetto di comprovati principi di sicurezza e nell'osservanza di chiare procedure di tracciabilità; quindi, di garantire: la corretta conservazione, la leggibilità del documento conservato nel tempo, l'accessibilità al singolo documento e la sua esibizione.

CNIPA resolution 2004 No. 11 defines the functions of the person responsible for electronic storage, describing in great detail the required tasks and responsibilities. In particular, this individual must create a computerized database of electronic documents in compliance with proven security principles and observance of clear tracking procedures, so as to ensure: proper maintenance; readability of documents stored over time; accessibility to the individual document and its display.

Il ruolo di Responsabile può essere anche demandato all'esterno e conferito a soggetti terzi. A volte, si tratta di veri e propri soggetti giuridici che diventano Responsabili della conservazione per diverse aziende; ovviamente, il vantaggio nella scelta di delegare verso l'esterno tale compito dipende dal volume dei documenti da portare in conservazione sostitutiva e dal *core business* dell'impresa interessata

This role can also be externally delegated and outsourced to third parties. Sometimes, legal professionals are responsible for storage for several companies; of course, the advantage in choosing to externally delegate this role depends on the volume of documents to be brought into electronic storage and on the *core business* of the company concerned.

****) Nelle more della pubblicazione definitiva del presente contributo è entrato in vigore in Italia Decreto Legislativo n. 235/2010 (pubblicato in Gazzetta Ufficiale n. 6 del 10 gennaio 2011), il quale contiene diverse modifiche al CAD. Le modifiche inserite nel testo non hanno inciso sostanzialmente su quanto riportato nel presente testo. L'unica modifica sostanziale riguarda l'introduzione in Italia di una nuova categoria d firma elettronica (accanto alla firma elettronica semplice, alla firma elettronica qualificata e alla firma digitale) e, cioè, la **firma elettronica avanzata**, definita dal legislatore come *l'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.*

****) While awaiting the final publication of the present contribution, Legislative Decree no. 235/2010 (published in the Gazzetta Ufficiale no. 6 dated 10 January 2010) has come into force in Italy. This decree contains various changes to the CAD. The changes made in the text have not had a significant impact on the contents of the present text. The only substantial modification relates to the introduction in Italy of a new category of electronic signature (besides the simple electronic signature, the qualified electronic signature and the digital signature), that is the **advanced electronic signature**, defined by the legislation as *all the data attached or connected with an electronic document which allows identification of the signatory of that document and guarantees the unique connection with the signatory, created using methods over which the signatory can maintain exclusive control, linked to the data to which the signature refers so that it is possible to detect whether the data has been modified subsequently.*

L'introduzione di tale nuova categoria di firma elettronica si è resa necessaria per garantire un allineamento con la normativa comunitaria attualmente in vigore (Direttiva 99/93/CE)

Avvertenze

Le informazioni fornite rivestono, in ragione dell'esigenza divulgativa dell'opera, un carattere orientativo e sommario e non mirano ad aiutare a risolvere i casi concreti e tipici della dematerializzazione documentale, la quale ha una grande complessità normativa e tecnica.

Prima di intraprendere un progetto di digitalizzazione è sempre e comunque indispensabile rivolgersi a soggetti giuridici specializzati e interpellare un consulente tributario e/o un avvocato esperto del settore.

Ogni singola normativa riportata può aver subito delle modifiche o abrogazioni da quando il testo è stato pubblicato.

The introduction of this new category of electronic signature has become necessary in order to guarantee alignment with current community legislation (Directive 1999/93/EC)

Disclaimer

The communicative requirements of this work mean that the information contained provides a summary and guidelines and it does not seek to help solve concrete and typical cases of the computerization of documents, which is legally and technically highly complex.

Before undertaking a digitization project, it is always essential to approach legal entities and consult a specialist tax adviser and / or a lawyer who is an expert in the field.

Each individual reported piece of legislation may have been amended or repealed since this text was published.

Spain

Author:

Alberto Olivares Antolín, CISA
IT Risk & Assurance Manager

Ernst & Young, S.L.
Calle Ibáñez de Bilbao, 28, 3ª Planta,
48009, Bilbao, Spain

E-Mail: Alberto.OlivaresAntolin@es.ey.com

Teléfono: +34 944 243 777

El presente artículo trata de posicionar y dar a conocer al lector el ámbito legislativo español respecto a la facturación electrónica ya que, de todos los documentos fiscales, es el único que dispone de un desarrollo normativo excelso para su tratamiento en cualquier tipo de soporte (papel y digital).

This article aims to offer the reader insight into Spanish legislation as regards electronic invoicing because, of all the fiscal documents, this is the only one to which in-depth legislative procedures apply for use in any format type (hard copy and digital).

1. Normativa reguladora de la factura electrónica

Este punto está dedicado a ofrecer al lector el marco normativo en que se apoya actualmente la factura electrónica en España:

- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (BOE 29 diciembre 2007)
- Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.
- ORDEN EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación electrónica y conservación electrónica de facturas, contenidas en el RD 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.

1. Electronic invoice regulations

This section is designed to outline the regulatory framework for electronic invoicing in Spain:

- Law 56/2007, of 28 December, on Measures to Promote the Information Society (Spanish Official Gazette 29 December 2007)
- Royal Decree 1496/2003, of 28 November, approving the regulations governing invoicing requirements.
- Order of the Department of Economy and Finance 962/2007, of 10 April, which develops certain provisions related to online invoicing and electronic invoice storage, contained in Royal Decree 1496/2003, of 28 November, approving the regulations governing invoicing requirements.

- ORDEN PRE/2971/2007, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares.
- Resolución de 24 de octubre de 2007, de la Agencia Estatal de la Administración Tributaria, sobre procedimiento para la homologación de software de digitalización contemplado en la Orden EHA/962/2007, de 10 de abril de 2007.

Estas normas se pueden consultar en la siguiente URL tanto en castellano como en inglés:
http://www.facturae.es/Documentacion/Normativa/FacturaElectronica/

- Presidential Order 2971/2007, of 5 October, on submitting invoices by electronic means when the recipient is the Civil Service or public organizations related to or subsidiary thereof, as well as filing invoices issued between private individuals with the Civil Service or public organizations related to or subsidiary thereof.
- State Tax Administration Agency Resolution of 24 October 2007, regulating the procedure for the homologation of digitalization software pursuant to Order/962/2007 of the Department of Economy and Finance, of 10 April 2007.

These standards can be viewed at the following URL both in Spanish and English:

http://www.facturae.es/Documentacion/Normativa/FacturaElectronica/

2. Conservación de Facturas y Documentos

Tanto para soporte papel como para soporte electrónico (admitido siempre y cuando los datos almacenados conserven fielmente su contenido original) la Agencia Tributaria (www.aeat.es) manifiesta que los empresarios y profesionales tienen el deber de conservar, durante el plazo fijado en la Ley General Tributaria para proceder a la inspección del Ejercicio los siguientes documentos según indica el artículo 19 de Reglamento por el que se regulan las obligaciones de facturación (Real Decreto 1496/2003, de 28 de noviembre), atendiendo al tipo de procedimiento:

- Las facturas o documento sustitutivo que hayan emitido.
- Las copias y matrices de las facturas expedidas conforme al artículo 2.1 y 2 del Reglamento citado por el que se regulan las obligaciones de facturación y la copias de los documentos sustitutivos expedidos.

2. Storage of Invoices and Documents

The Tax Agency (www.aeat.es) states that employers and professionals are obliged to store the following documents in both hard copy and electronic format (as long as the data stored is faithful to the original), for the period stipulated in the General Tax Law for fiscal auditing purposes in accordance with Article 19, approving the regulations governing invoicing requirements (Royal Decree 1496/2003, of 28 November) according to the type of procedure:

- Any invoices or replacement documents issued.
- Any invoice copies or originals issued in compliance with Article 2.1 and 2 of the aforementioned regulations by means of which the invoicing requirements and copies of the replacement documents sent are regulated.

- Las facturas expedidas de acuerdo con el artículo 2.3 del citado Reglamento, así como sus justificantes contables.
- Los recibos justificativos del reintegro de la compensación del régimen especial de la agricultura, ganadería y pesca, tanto el original de aquél, por parte de su expedidor, como la copia, por parte del titular de la explotación.
- Los documentos acreditativos del pago del impuesto a la Importación.

- Any invoices sent in accordance with Article 2.3 of the aforementioned Regulations, as well as any supporting accounting documents.
- Supporting receipts for the repayment of the agriculture, farming and fishing special funding, both in the original copy from the issuer and the farm owner's copy.
- Import tax payment supporting documents.

Por otro lado, el artículo 30 del Código de Comercio vigente establece una obligación para los empresarios de conservar libros, correspondencia, documentación y justificantes concernientes a su negocio durante **seis años**, a partir del último asiento realizado en los libros. Pero va más allá, y según este mismo artículo, en el caso de fallecimiento del empresario, traslada esta obligación a sus herederos legales. Y para el caso de disolución de la sociedad, traslada la obligación a los liquidadores.

Furthermore, Article 30 of the current Commercial Code stipulates employers' obligations to retain accounting records, correspondence, documentation and supporting documents concerning their business for a period of six years from the date of the last entry made in the accounts. It is, however, more far reaching than that and according to the above Article, in case of the death of the employer, the obligation is transferred to his legal heirs. In the event of dissolution of the company, the obligation passes onto the liquidators.

A nivel fiscal se requieren cuatro años contados a partir de la finalización del período voluntario de ingreso de la deuda correspondiente a cada impuesto, o de la presentación de la declaración de que se trate. Aún así, la ley de Impuesto de Sociedades establece, en caso de que existan bases imponibles negativas acreditadas o compensadas, la obligación de justificar la procedencia y cuantía de las mismas, aunque se hubieran generado fuera del período de prescripción (el plazo de compensación de estas bases es de 15 años). Además, según una reciente modificación del Código Penal, un Tribunal que juzgue una causa penal podría llegar a pedir documentación de hasta 10 años máximo de antigüedad.

On a fiscal level, the period required is four years starting from the end of the voluntary period for settlement of the tax due, or from the submission of the relevant declaration. evertheless, Corporate Tax law states that in the event that there are negative tax bases credited or offset, there remains the requirement to justify the origin and quantity of these negative tax bases, even if they were generated outside the limitation period (the offset period of these bases is 15 years). Moreover, following a recent amendment to the Penal Code, a Tribunal presiding over criminal proceedings may request documentation dating back to a maximum of 10 years.

Es importante tener en cuenta que dichos documentos deberán conservarse en cualquier lugar dentro del territorio nacional (a excepción de las facturas que podrían residir en formato electrónico en cualquier país de la UE).

It is important to bear in mind that these documents will have to be stored somewhere on national soil (with the exception of invoices that may be saved in electronic format in an EU country).

En caso de ser otro país, tal obligación únicamente se considerará válidamente cumplida si se realiza mediante el uso de medios electrónicos que garanticen el acceso en línea bajo autorización previa de la Agencia Estatal de Administración Tributaria. (Artículo 22 1496/2007)

In the case of another country, this requirement shall only be considered as duly fulfilled if carried out through the use of electronic methods that guarantee online access on prior authorization from the State Tax Administration Agency. (Article 22 1496/2007)

Los requisitos de conservación temporal son idénticos para cualquier tipo de soporte. El artículo 20 de Decreto 1496/2003 indica que los documentos señalados anteriormente se deberán conservar de forma que se garantice el acceso a ellos por parte de la Administración tributaria sin demora, salvo causa debidamente justificada. Esta obligación podrá cumplirse mediante la utilización de medios electrónicos.

The requirements for temporary storage are identical for all format types. Article 20 of Decree 1496/2003 indicates that the documents mentioned above must be stored in such a way as to guarantee access to the tax authority without delay, unless duly justified. This requirement may be met by electronic means.

2.1. Cómo se conservan electrónicamente facturas recibidas en papel

2.1. How to store paper invoices electronically

Aunque normativamente se prevé la conservación electrónica de facturas, por la condición de que las facturas deban estar disponibles para la inspección tributaria en el formato original en el que fueron recibidas, hasta muy recientemente se entendía que dicha conservación electrónica solo aplica a las facturas remitidas electrónicamente.

Although the regulations provide for electronic storage of invoices on condition that the invoices are available for tax auditing in the original format in which they were received, it has generally been understood that until very recently this so-called electronic storage applies exclusively to invoices that are sent electronically.

La Agencia Tributaria (sección factura electrónica) está promoviendo actualmente el concepto de Digitalización Certificada como el proceso en que, partiendo de una factura en papel, se genera una imagen digital firmada electrónicamente a la que se le admite tener el mismo valor probatorio que la factura original, de forma semejante a la de una compulsa electrónica permitiendo, por ello, destruir la propia factura original en papel.

The Tax Agency (electronic invoice department) is currently promoting the concept of Certified Digitization as a process by which an electronically signed digital image is produced from a paper invoice and is legally valid as an original. This is similar to a digitally authenticated copy and it means that the paper invoice can be destroyed.

Para que se dé por buena la presunción descrita, es preciso utilizar dispositivos auditados (lo que, en definitiva, supone una modalidad de homologación) así como disponer de un informe de auditoría del proceso de digitalización.

In order for the above proposal to be authorized, it is essential to use certified devices (which basically consists of a homologation procedure), as well as to have an audit report of the digitization process.

El detalle sobre el proceso de homologación, y las características a cumplir por el software de digitalización, se encuentra descrito en la Resolución de 24 de octubre de 2007, de la Agencia Estatal de Administración Tributaria, sobre procedimiento para la homologación de software de digitalización contemplado en la Orden EHA/962/2007, de 10 de abril de 2007.

The details of the homologation process and the features to be contained in the digitization software are described in the Resolution of 24 October 2007 of the State Tax Administration Agency, regulating the procedure for the homologation of digitalization software pursuant to Order/962/2007 of the Department of Economy and Finance, of 10 April 2007.

Para garantizar que los documentos así digitalizados cumplen de forma íntegra las condiciones de autenticidad, se recomienda utilizar la modalidad de firma electrónica ES-X-L, descrita anteriormente como firma completa, ya que quien deba verificar la firma no debe preocuparse de encontrar el mecanismo de comprobación de validez, que puede ser diferente para cada prestador. Debe tenerse en cuenta que solo en España existen más de 20 sistemas de certificación, cada uno de los cuales tiene su propio mecanismos de verificación.

In order to guarantee that documents that have been digitalized in this way fully meet the authenticity requirements, it is recommended that the electronic signature ES-X-L is used. This has previously been referred to as the complete signature, as anyone responsible for checking the signature does not have to concern themselves with finding the validity verification mechanism, which could potentially be different for each provider. It is important to note that there are more than 20 certification systems in Spain alone, each of which has its own verification mechanism.

Si se emplea un sistema OCR (Optical Character Recognition) el sistema puede reconocer letras y números y superponerlos en una capa del fichero, de forma que se simplifica la indexación y la búsqueda de documentos. Si además la factura se ha impreso según una plantilla acordada, el OCR permitirá codificar la factura en el formato estándar UBL (promovido por el consorcio internacional Oasis), facilitando también la inserción del contenido de la factura en el sistema informático y su tratamiento más o menos automatizado.

If an OCR (Optical Character Recognition) system is implemented, it may recognize letters and numbers and superimpose them on a file header, thus simplifying documentation indexing and search. Also, if the invoice has been printed using an authorized template, the OCR will enable the invoice to be encoded in the standard UBL format (endorsed by the International Consortium Oasis), thus facilitating the insertion of the invoice details in the IT system and its authorized use.

Para minimizar el número de modelos posibles y mejorar las probabilidades de reconocimiento óptico, existen varias iniciativas. Una de ellas es UNeDocs, de las Naciones Unidas, pensada para facturas complejas utilizas en intercambios de importación y exportación, donde seguramente es más necesaria por las dificultades añadidas por los múltiples idiomas utilizados en un tránsito de mercancías.

There are various initiatives in existence to minimize the number of possible templates and improve the probability of optical recognition. One of these is the United Nations' UNeDocs, designed for complex invoices used in import/export exchanges, where the need is even greater due to the added difficulty of multiple languages used in the transit of goods.

Otra iniciativa es la Factura Normalizada de ASIMELEC. La factura normalizada es una plantilla que facilita la emisión de facturas, y su posible digitalización por el receptor.

Another initiative is ASIMELEC's Standardized Invoice. The standardized invoice is a template that facilitates the invoicing process and its potential digitization by the recipient.

2.2. Cómo se conservan en papel las facturas recibidas electrónicamente

Aunque existe la posibilidad de almacenar facturas electrónicas en papel mediante un código de barras PDF-417, es posible otro mecanismo alternativo.

Si existen aplicaciones informáticas que gestionen un repositorio de facturas emitidas o recibidas, según corresponda, junto con la firma electrónica generada o verificada, proporcionando un código de autenticación de mensajes asociado a cada factura, cabe la posibilidad de identificar las facturas mediante dicho código.

Este código permitirá el acceso al documento asociado existente en el repositorio y garantizará, al que accede, que la factura cumple con los requisitos contemplados en la normativa.

Por tanto, una factura transcrita al papel con este código es válida, siempre que se mantenga dicho repositorio donde exista la factura y su firma electrónica, exista un mecanismo de verificación de la firma en el repositorio y se pueda acceder de forma completa a la factura mediante dicho código electrónico de autenticación.

Esta modalidad de gestión de facturas electrónicas en papel está prevista en el Artículo 6 de la Orden EHA-962/2007.

2.2. How to store invoices received electronically in paper format

Despite the fact that it is possible to store electronic invoices in paper format using a PDF-417 bar code, this is also another alternative.

If IT applications are available that manage a database of both sent and received invoices together with the generated or verified electronic signature and which assign an authentication code for messages associated to each invoice, it is possible that the invoices can be identified using this code.

This code allows access to the associated document in the database and will guarantee that the invoice meets the requirements outlined in the regulations.

As such, any invoices that are transcribed onto paper with this code are valid as long as the database containing the invoice and its electronic signature is maintained. There also has to be a verification mechanism for the signature in the database and it must be possible to fully access the invoice by means of the electronic authentication code.

This management method for electronic invoices on paper is provided for in Article 6 of Order 962/2007 of the Department of Economy and Finance.

3. Facturación y Correo Electrónico

Podemos afirmar que una gran mayoría de las empresas en España utilizan el correo electrónico para el envío de sus facturas. Lo curioso es que “de facto” se considera que esta práctica es correcta. Sin embargo, si se analiza la normativa se puede observar la incorrección de esta consideración.

La empresa que envía facturas tradicionales por correo electrónico lo único que pretende es hacerla llegar más rápidamente al destinatario, reduciendo el período de maduración y acortando el plazo del cobro, pero también traslada a su cliente los costes inherentes a la impresión de las facturas (papel, tinta / tóner, consumo eléctrico, etc.) que antes no tenía.

3. Email and Invoicing

It is worth noting that the vast majority of companies in Spain use email to send their invoices. The interesting thing is that this practice is considered to be correct “de facto”. However, closer analysis of the regulations reveals that this view is actually incorrect.

A company that sends conventional invoices by email has the sole intention of ensuring that they reach the recipient more quickly, therefore reducing the payment terms. They are also passing on the cost of printing the invoices to the client, which are costs the client did not have before (paper, ink / toner, electricity).

La Dirección General de Tributos se ha pronunciado en diferentes ocasiones sobre este tema. Citemos como por ejemplo la Consulta nº 1037-03 (25/7/2003) que aclara que:

"El mero hecho de enviar una factura en formato fichero mediante correo electrónico no confiere la condición de factura electrónica, al no cumplirse los requisitos exigibles a este tipo de facturas."

Asimismo, el propio preámbulo de la Orden EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el reglamento por el que se regulan las obligaciones de facturación (BOE del 14), dice literalmente:

"La generalización del uso de las telecomunicaciones y del correo electrónico para la remisión de todo tipo de mensajes, incluidos entre ellos el envío de las facturas o documentos sustitutivos, hace necesario aclarar la validez legal de los remitidos en formato electrónico al destinatario, debiendo aceptarse esta práctica como válida en la medida que, como ya se ha indicado, incorpore medios que garanticen la autenticidad de su origen y la integridad de los documentos así remitidos."

Se puede afirmar, por tanto, que el mero hecho de enviar facturas por correo electrónico sin ningún medio que garantice los requisitos exigidos en el régimen de facturación telemática (autenticidad e integridad), no es válido a efectos fiscales.

Para poder utilizar el correo como medio de transmisión de la factura con validez a efectos fiscales, se tendrían que dar las siguientes circunstancias:

- En primer lugar, disponer del consentimiento expreso del destinatario (verbal o escrito, mejor escrito que verbal) para poder hacerlo.

The Directorate General for Taxation has addressed this matter on a number of occasions. Take, for example, Query no. 1037-03 (7/25/2003) which clarifies that:

"The mere fact of sending an invoice in file format by email is not tantamount to an electronic invoice, as it does not meet the requirements for these types of invoice."

Likewise, the preamble of Order 962/2007, of 10 April, of the Department of Economy and Finance, which develops certain provisions related to online invoicing and electronic invoice storage, contained in Royal Decree 1496/2003, of 28 November, approving the regulations governing invoicing requirements (Official Spanish Gazette from the 14th), states:

"The general use of telecommunications and email for sending all types of message, including those containing invoices or replacement documents, has given rise to the need to clarify the legal validity of the documents sent in electronic format to the recipient. As already indicated, this practice is only considered valid on the condition that the authenticity of origin and integrity of the documents sent in this manner are guaranteed."

It follows then that the mere act of sending invoices by email without any means of guaranteeing the requirements laid down for electronic invoicing (authenticity and integrity) is not valid for fiscal purposes.

In order to use email as a valid means of sending invoices for tax purposes, the following conditions must be met:

- Firstly, the sender must have received the express consent of the recipient (verbal or written, preferably written).

- Utilizar una herramienta que le haga cumplir con los mencionados requisitos, que bien podría ser firmando electrónicamente la factura que se enviaría como anexo al correo electrónico, o bien, firmando electrónicamente el propio correo. Este último caso obligaría a tener que conservar el propio correo con su factura anexada en lugar de la propia factura.
- En el momento de firmar la factura o el correo electrónico, habría que incorporar un sello de tiempo de la entidad expedidora del certificado utilizado en la firma que acredite la validez de dicho certificado. De esta manera, el destinatario no quedará obligado a verificar su validez por acceso y consulta de las listas de certificados revocados llevada por la entidad prestadora de los servicios de certificación, aunque sí que debe verificar la firma del sello.
- De no incorporar el anterior sello, el expedidor podría igualmente enviar la factura firmada sin dicho requisito, pero tendría que poner a disposición del destinatario de la misma el correspondiente mecanismo de verificación y de validación del certificado electrónico utilizado en el momento de la firma.

- Appropriate software must be used in order to comply with the aforementioned requirements, enabling the invoice to be stamped with an electronic signature; alternatively the email itself can be signed electronically. In the case of the second option, the email will have to be archived with the invoice attached instead of the invoice alone.
- On signing the invoice or email, a signature certificate time stamp of the issuer will have to be incorporated in order to verify the validity of the certificate. The recipient will therefore not have to check its validity by accessing and consulting the lists of repealed certificates by the certification service provider, although it will be necessary to check the signature stamp.
- The sender may also send the signed invoice without the aforementioned stamp; however they will have to make the electronic certificate validation and verification mechanism used for the signature available to the recipient.

4. Admisibilidad y Nivel Probatorio de la Factura Electrónica

La Jurisprudencia Española ha exigido a los documentos electrónicos (para atribuirles el carácter de documento) que quede asegurada la procedencia y veracidad de su autoría así como la autenticidad de su contenido, que siempre se puede lograr plenamente en sede de reconocimiento judicial con la asistencia, en su caso, de peritos expertos en la materia.

Según lo expuesto anteriormente, el documento informático puede presentarse como medio de prueba en un procedimiento siendo el reconocimiento judicial el que proporcione la información sobre su validez y eficacia, teniendo en cuenta que, de acuerdo con lo especificado en el artículo 356 de la Ley de Enjuiciamiento Civil (L.E.C.).

4. Eligibility and Probative Level of Electronic Invoices

Spanish Case Law has required that electronic documents are assured as regards their origin, veracity of authorship, and authenticity of content (in order to ascribe the nature of the document). This should be readily ascertained by means of legal inspection with the help of expert opinions, where necessary.

As mentioned above, the digital document may be required as evidence in legal proceedings, with the legal inspection offering information on its validity and efficacy in accordance with the provisions of Article 356 of the Civil Procedure Act.

Los documentos firmados electrónicamente, a los que la más reciente legislación equipara a "documentos" (en el sentido tradicionalmente admitido) a día de hoy y desde un punto de vista procesal, se los asimila a la prueba documental.

Y son precisamente, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica las que de un modo más claro, realizan a efectos procesales probatorios, la equiparación entre ambos tipos de documentos.

La Ley 59/2003, de 19 de diciembre, de Firma Electrónica dispone en el artículo 3.8 a propósito de los documentos electrónicos (entre los que enmarcamos a la Factura Electrónica) que el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio.

Si tenemos en cuenta la equiparación que la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, hace de la firma electrónica respecto a la manuscrita, los documentos electrónicos deben regirse por el régimen procesal de la prueba documental.

Esta Ley de Firma Electrónica, emplea los mismos criterios de distinción entre documento público y documento privado, que se emplean en el Código Civil y en la Ley de Enjuiciamiento Civil, a la hora de distinguir la naturaleza de estos tipos de documentos.

Por tanto, la cuestión del valor y la eficacia jurídica de la Factura Electrónica como medio probatorio, queda clara, a través del artículo 299,2 de la L.E.C. y del artículo 3, 8 de la Ley 59/2003 de 19 de diciembre de Firma Electrónica, en virtud de los cuales, artículo 299, 2: "También se admitirán, conforme a lo dispuesto en esta Ley, (…) los instrumentos que permitan archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso". Y según el mencionado artículo 3, 8 de la Ley 59/2003: "El soporte en el que se hallen los datos firmados electrónicamente, será admisible como prueba documental en juicio".

Electronically signed documents, which current legislation today equates to "documents" (in the traditional sense of the term), amount to documentary evidence from a legal proceedings point of view.

More precisely, it is Law 34/2002, of 11 July, governing the services of the information society and electronic commerce and Law 59/2003, of 19 December, regulating Electronic Invoices, that clarify the equivalency between the two types of document most clearly for probative procedural purposes.

With regards to electronic documents (among those which have been included in the Framework for Electronic Invoices), Article 3.8 of Law 59/2003, of 19 December, governing Electronic Signatures, states that the format in which the electronically signed data is to be found shall be admissible as documentary evidence in a court of law.

If we take into account the approximation that Law 59/2003, of 19 December, on Electronic Signatures makes of the electronic signature to the manuscript itself, electronic documents are governed by the procedural framework of documentary evidence.

This Law on Electronic Signatures employs the same distinction criteria between public and private documents that are used in the Civil Code and the Civil Procedure Act when distinguishing the nature of these types of document.

Therefore, the question of the value and legal efficacy of the Electronic Invoice as a probative medium is clarified in Article 299.2 of the Civil Procedures Act and Article 3.8 of Law 59/2003 of 19 December on Electronic Signatures, in reference to which Article 299.2 states that: "In accordance with the provisions in this act, any tools that allow storage, access to or reproduction of words, data, figures and mathematical calculations carried out for accounting or other purposes that are relevant to the process (…) shall be admissible". Furthermore, according to Article 3.8 of Law 59/2003: "The format in which electronically signed data is contained shall be admissible as documentary evidence in a court of law."

Cuando la parte a quien interese la eficacia de un documento electrónico, lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en la Ley 59/2003. Esto es, para impugnar una Factura Electrónica avalada por Firma Electrónica, será necesario comprobar, que por el prestador de servicios de certificación, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta respecto de la firma, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información emitida y la identidad de los firmantes.

5. Requisitos técnicos de facturas electrónicas

Lo expuesto a continuación es aplicable a los países miembros de la Unión Europea. Para otros Estados, es necesaria la autorización de la Agencia Estatal de Administración Tributaria (AEAT).

Las facturas electrónicas se pueden emitir en diferentes formatos (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg o txt, entre otros) siempre que se respete el contenido legal exigible a cualquier factura y que se cumplan ciertos requisitos para la incorporación de la firma electrónica reconocida que cumpla lo establecido por la Directiva de Firma Electrónica (la Ley 59/2003, en el caso de los prestadores españoles).

El reglamento establece la existencia de dos formas diferentes de intercambiar documentos electrónicos a las que se les presume un nivel de fiabilidad alto, sin descartar, a priori, otras opciones tecnológicas siempre y cuando tengan el reconocimiento de la Agencia Tributaria. Estas dos formas son: Por un lado el empleo de una firma electrónica y por otro el uso de sistemas EDI. Estas dos formas garantizan la autenticidad e integridad que son los verdaderos requisitos que se exigen a los documentos.

El proceso de facturación electrónica lo forman dos procesos básicos y diferenciados que corresponden a cada interlocutor:

When a party affected by the efficacy of an electronic document requests or challenges its authenticity, the provisions of Law 59/2003 shall apply. This means that in order to contest an Electronic Invoice certified by Electronic Signature, it will be necessary to check that all the requirements established in the law are met on the part of the certification service provider. These will include the service guarantee provided as regards the signature and, in particular, the obligations of guaranteeing the confidentiality of the process as well as the authenticity, storage and integrity of the information issued and the identity of the signatories.

5. Electronic Invoice Technical Requirements

The following information is applicable to members of the European Union. For other countries, authorization from the State Tax Administration Agency (AEAT) must be obtained.

Electronic invoices may be issued in various formats (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg or txt, to name but a few) as long as they contain all the content required by law for all invoice types, and that they meet specific requirements for the incorporation of a recognized electronic signature that complies with the provisions of the Electronic Signature Directive (Law 59/2003, in the case of Spanish providers).

The regulations recognize two forms of the exchange of electronic documents that are considered to be particularly reliable, without ruling out, a priori, other technological options as long as they are authorized by the Tax Agency. These two forms consist of the use of an electronic signature on the one hand, and the use of EDI systems on the other. They both guarantee authenticity and integrity, which are the fundamental requirements for the documents.

The electronic invoicing process comprises two basic processes that are distinct for each party:

- El emisor, con la conformidad del receptor, transmite a éste por medios telemáticos la factura electrónica (que incluye una firma electrónica) y conserva copia o matriz (la base de datos). No es necesario conservar los documentos electrónicos firmados.
- El receptor, recibe la factura en formato digital y la conserva en soporte informático, en el formato en el que lo recibió, para su futura consulta e impresión, si fuera necesario. Al ser la factura un documento firmado electrónicamente, debe guardar la información relativa a la comprobación de la validez de la firma electrónica.

Por tanto, es importante analizar si la empresa va a iniciar la implantación desde el punto de vista de emisor, desde el punto de vista de receptor de facturas o desde una posición mixta.

A pesar de que la implantación de la factura electrónica implica necesariamente a ambas partes (al emisor y al receptor) la gran mayoría de los proyectos que se inician en España están siendo orientados a la posición de emisión de facturas.

Para el emisor se exige:

- Tener el consentimiento previo del receptor.
- Garantizar la autenticidad del origen y la integridad de las facturas, mediante el uso de la firma electrónica reconocida.
- Almacenar copia de las facturas. Este requisito no es necesario si se puede reconstruir una factura a partir de la información guardada en la base de datos de la empresa.
- Las facturas almacenadas deben contener determinados elementos que faciliten su búsqueda, visualización e impresión en caso de inspección (acceso completo y sin demora a los datos).

- The issuer or sender sends the electronic invoice to the recipient, with their agreement, by electronic means (including the electronic signature) and keeps a copy of the original (in their database). It is not necessary to store the signed electronic documents.
- The recipient receives the invoice in digital format and saves it in the same format for future consultation and printing where necessary. Should the invoice consist of an electronically signed document, they will need to save the information on the electronic signature validity check.

It is therefore important to ascertain whether the company intends to implement the process initially from the point of view of the issuer, the recipient or both.

Despite the fact that the production of an electronic invoice involves both parties (the issuer and the recipient), the vast majority of projects initiated in Spain target the invoice issuer.

The issuer is expected to:

- Obtain the prior consent of the recipient.
- Guarantee the authenticity of the origin and integrity of the invoices through the use of a recognized electronic signature.
- Keep a copy of the invoices issued. This requirement is not mandatory if it is possible to reproduce an invoice based on the information saved in the company's database.
- Any invoices that are archived must contain specific elements that facilitate search, visualization and printing in the event of an audit (full and immediate access to the data).

En el proceso de recepción de facturas mediante la utilización de la factura electrónica, se busca habitualmente la integración con los ERPs. La complejidad en este proceso radica en la necesidad de tratar con un número indeterminado de formatos electrónicos y de prestadores que emiten certificados que se usan en las firmas electrónicas de las facturas, junto con la recepción de facturas en papel.

Para disminuir la complejidad del proceso, se puede optar por la modalidad de auto-facturación, en la que el propio receptor controla el formato de recepción y garantiza la conciliación contable. En este caso debe existir un acuerdo entre el emisor y el receptor para dar por bueno este procedimiento. También este enfoque será preferible en entornos de facturación internacional en el que el emisor de la factura tenga dificultades para cumplir la normativa española. Otra posibilidad a considerar por las empresas receptoras es el uso de plataformas externas, que, bajo la modalidad de facturación por terceros, facilitarán todo el proceso de transformación de las facturas e incluso la digitalización certificada de los documentos recibidos en papel.

Para el receptor se exige:

- Disponer del software necesario para la validación de la firma electrónica (la parte más compleja).
- Almacenar las facturas recibidas digitalmente (factura y firma) en su formato original.
- Las facturas almacenadas deben contener elementos que faciliten su búsqueda, visualización e impresión en caso de inspección (acceso completo y sin demora a los datos).

La posibilidad de delegar la ejecución material de la facturación, bien en los destinatarios de las operaciones (auto factura), bien en terceros mediante la contratación de sus servicios (facturación por terceros) se reconoce expresamente en la normativa actual (ver artículos 5 y 19.3 del Real Decreto 1496/2003). El hecho de delegar la facturación en terceros no exime de responsabilidad, por lo que los obligados tributarios deberán ser cuidadosos en la elección de su proveedor.

Integration with the ERPs forms a common aspect of the reception process of invoices through the use of electronic signatures. The complexity of this process lies in the need to handle an unspecified number of electronic formats and providers issuing certificates for the invoice electronic signatures, alongside the reception of paper invoices.

To simplify the process, it is possible to opt for the self-invoicing method in which the recipient controls the format used for the invoice and guarantees the reconciliation of accounts. In this case, there must be an agreement in place between the issuer and recipient in order to implement this procedure. This approach will also be preferable in an international invoicing backdrop, where the issuer may have difficulty meeting Spanish regulations. Another possibility to consider for recipient companies is the use of external platforms which, under the third-party invoicing method, facilitate the entire invoice transformation process and even the certified digitization of documents received in paper format.

The recipient is expected to:

- Have the necessary software for validating the electronic signature (the most complex part).
- Store the digitally received invoices (invoice and signature) in their original format.
- Any invoices that are archived must contain elements that facilitate search, visualization and printing in the event of an audit (complete immediate access to the data).

The possibility of delegating the task of producing the invoice material either to the recipient (self-invoicing) or to third parties through contracting their services (third-party invoices) is expressly provided for in current legislation (see Articles 5 and 19.3 of Royal Decree 1496/2003). The act of delegating the invoicing process to third parties does not release the taxpayer from his duty to be careful in the choice of provider.

Para que la delegación de la facturación sea válida, deberán cumplirse los siguientes requisitos:

- Acuerdo previo documentado por escrito entre el obligado tributario emisor y la entidad que efectivamente gestione la expedición de la factura, ya sea un tercero o el obligado tributario receptor (auto factura). En el citado acuerdo constará de manera expresa la autorización del obligado tributario emisor y las operaciones comprendidas en el acuerdo.
- El empresario o profesional que delega la emisión de facturas en el destinatario de las mismas deberá aceptar o rechazar la emisión de cada factura concreta, para lo que dispondrá de quince días desde la recepción de la copia o su acceso telemático a ella. El rechazo deberá ser expreso. Si se produce este rechazo, la factura se anula, o se tiene por no emitida. Estas facturas serán expedidas en nombre y por cuenta del empresario o profesional que haya suministrado los conceptos que en ellas se documentan.
- Asignar una serie específica por cada entidad que gestiona facturas por cuenta del obligado emisor.

Una interesante posibilidad que aparece con la Orden EHA 962/2007 es la de convertir facturas en papel en facturas electrónicas por parte del tercero que gestiona la expedición electrónica. Aplicar las previsiones de la Orden EHA 962/2007 que contempla la Digitalización Certificada llevada a cabo al firmar electrónicamente las facturas digitalizadas o escaneadas por el propio receptor, y sin necesidad de acuerdo previo con el emisor. En este caso, es necesario cumplir ciertos requisitos en los procesos de digitalización, que puedan ser auditados, y que permitan confiar en que el proceso se llevará a cabo respetando rigurosamente el contenido de los documentos en papel originales.

In order for the delegation of the invoicing process to be valid, the following requirements must be met:

- Prior documented agreement between the taxpayer and the party that manages the invoicing procedures – either a third party or the recipient (self-invoicing). The aforementioned agreement shall expressly include the authorization of the issuing party and the operations covered by the agreement.
- Any employer or professional who transfers the invoicing process to the recipient will have to accept or reject the production of each invoice. They will have fifteen days from the date of receipt of their copy or online access in which to do so. Rejection must be expressed. It is then null and void or is not issued. These invoices will be sent in the name of and on behalf of the employer or professional who supplied the documented information.
- A specific serial number will have to be assigned for each party that manages the invoice process on behalf of the sender.

A useful possibility contained in Order 962/2007 of the Department of Economy and Finance is that of converting paper into electronic invoices by a third party managing the electronic invoicing procedure. Order 962/2007 of the Department of Economy and Finance provides for Certified Digitization on the electronic signature of digital or scanned invoices by the recipient themselves, without prior agreement from the issuer. In this case, certain requirements will have to be met in the digitization processes, which may be subject to auditing, and which must guarantee that the process will be carried out with strict adherence to the content of the original paper documents.

Además los sistemas técnicos utilizados deberán facilitar la firma electrónica en la fase más temprana de la digitalización que sea posible, lo que se deberá acreditar igualmente con un proceso de auditoría, que podrá ser obtenido por el fabricante.

Si el proceso se sigue con todos los requisitos, es posible destruir las facturas en papel, una vez concluido el proceso de su digitalización certificada.

6. Se puede realizar la conservación de facturas electrónicas en el extranjero?

La conservación de facturas en el extranjero, se encuentra recogida en el Artículo 9 de la Orden EHA/962/2007. También se hace mención en los Artículos 19 y 22 del Real Decreto 1496/2003.

Tanto el emisor como el destinatario de la factura, pueden decidir si la conservación se hace en España o en el extranjero. Pero sólo es válida la conservación en el extranjero de las facturas en formato electrónico para garantizar el acceso completo y sin demora injustificada.

Los Artículos citados anteriormente normalizan el procedimiento para la admisión, por parte de la Agencia Estatal de Administración Tributaria (AEAT), de la conservación de facturas en el extranjero:

- Si se hace en un país de la UE o país con el que exista un instrumento jurídico de asistencia mutua:
  - Puede hacerlo directamente el obligado tributario.
  - Es necesaria comunicación previa a la Agencia Estatal de Administración Tributaria (Art. 22-2 RD 1496/2003).
  - Puede hacerlo a través de un tercero en nombre del destinatario de la factura o expedidor de la factura.
- Si el tercero es residente en España, o UE, o país con el que existe un instrumento jurídico, es necesaria comunicación previa a la Agencia Estatal de Administración Tributaria (Art. 22-2 RD 1496/2003).

Moreover, the technical systems used must enable electronic signature in the earliest possible stages of digitization. This must also be accredited via an auditing process and may be obtained from the provider.

If the process meets all the requirements, it is possible to destroy the paper copies of the invoices once the certified digitization process has been completed.

6. Can electronic invoices be conserved abroad?

Conserving invoices abroad is covered by Article 9 of Order EHA/962/2007. It is also mentioned in Articles 19 and 22 of Royal Decree 1496/2003.

Both the invoice issuer and addressee can request that it be conserved in Spain or abroad. However, conserving electronic invoices abroad is only permitted to guarantee full access to them without unjustified delay.

The articles mentioned above set the rules under which the AEAT (National Tax Administration Agency) permits invoices to be conserved abroad:

- If conserved in an EU member state or a country with a mutual legal assistance agreement:
  - The taxpayer may proceed.
  - S/he should first inform the AEAT (Article 22-2RD 1496/2003).
  - This can be done via a third party on behalf of the invoice issuer or addressee.
- If the third party is resident in Spain, the EU or a country with a mutual legal assistance agreement, the AEAT must be informed in advance (Art. 22-2 RD 1496/2003).

- Si el tercero no es residente ni en España, ni en la UE, ni país con el que existe un instrumento jurídico, es necesario autorización previa de la Agencia Estatal de Administración Tributaria (Art. 19-4 RD 1496/2003).
- Si se hace en un país extranjero distinto a los anteriores:
  - Puede hacerlo directamente el obligado tributario previa comunicación a la Agencia Estatal de Administración Tributaria. (Art. 9-2 Orden EHA 962/2007).
  - Puede hacerlo a través de un tercero.
  - En este caso es necesaria la autorización previa de la Agencia Tributaria (Art. 9-2 Orden EHA 962/2007).
  - Pueden pedir la autorización a instancias de empresarios o profesionales españoles. No a instancias de residentes en el extranjero, que pretendan homologar sus sistemas para prestar servicios a residentes en España.
  - El procedimiento está regulado en el Artículo 9-4 de la Orden EHA 962/2007.

- If the third party is not resident in Spain, the EU or a country with a mutual legal assistance agreement, prior authorization must be sought from the AEAT (Art. 19-4 RD 1496/2003).
- If conserved in a foreign country not covered by the above:
  - The taxpayer may proceed after first informing the AEAT. (Art. 9-2 EHA Order 962/2007).
  - This can be done via a third party.
  - In this case, prior authorization is required from the Tax Agency (Art. 9-2 Order EHA 962/2007).
  - Authorization may be sought on behalf of Spanish businesspeople or professionals. Not on behalf of residents abroad wishing to have their systems recognized to provide services to Spanish residents.
  - The procedure is regulated in Article 9-4 of Order EHA 962/2007.

6.1. ¿Qué condiciones tiene que cumplir la factura electrónica en el caso de que se genere por una empresa extranjera que ofrece su servicio o producto a un cliente español?

Está recogido en el Artículo 4 de la Orden EHA/962/2007 por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas.

Debe cumplir las mismas condiciones que tienen las facturas expedidas y remitidas en España.

Caso de uso de firma electrónica, es el cliente residente en España el que debe cerciorarse de que se trata de una firma electrónica reconocida. Esto se cumple en los siguientes casos:

Caso de Unión Europea cuando se cumpla alguno de los siguientes requisitos:

6.1. What conditions must electronic invoices meet if they are issued by a foreign company selling services or products to a Spanish client?

This issue is covered in Article 4 of Order EHA/962/2007, which sets out specific provisions on telematic invoicing and the conservation of electronic invoices.

These invoices must meet the same conditions imposed on invoices issued and sent in Spain.

The client resident in Spain must ensure that any electronic signature used is valid. This condition is satisfied in the following cases:

Within the European Union if one of the following requirements is met:

- El certificado indica en su propio contenido que es un certificado reconocido y la Autoridad de Certificación tiene públicamente accesibles sus políticas de certificación en las que indica que cumple con lo establecido en la Directiva europea de firma electrónica 1999/93/CE.
- El certificado se halle acreditado por una entidad establecida en la UE conforme a un Esquema Voluntario de Acreditación de acuerdo con lo recogido en la Directiva 1999/93/CE.
- El certificado se halle inscrito en algún registro público de autoridad competente en materia de firma o fiscal.

Caso países fuera de la Unión Europea cuando se cumpla alguno de los siguientes requisitos:

- El certificado se halle acreditado por una entidad establecida en la UE conforme a un Esquema Voluntario de Acreditación de acuerdo con la Directiva 1999/93/CE.
- Que una entidad AC establecida en la UE avale el certificado.
- Que el certificado esté reconocido en virtud de acuerdos de la UE con terceros países.

6.2. ¿Se pueden expedir facturas electrónicas desde fuera de España, en nombre de empresas residentes en España?

La expedición de facturas fuera del territorio español, se encuentra recogido en el Artículo 9 de la Orden EHA/962/2007. Asimismo, en el Artículo 5 del Real Decreto 1496/2003 del Reglamento que regula las obligaciones de facturación.

Si el tercero, o destinatario caso auto factura, que expide facturas no es residente en España, pero es residente en un país de la UE o país con el que exista un instrumento jurídico:

- The certificate's content indicates that it is a valid certificate and that the Certification Authority makes its certification policies publicly accessible and that said policies state that they satisfy the provisions of the European Electronic Signature Directive 1999/93/EC.
- The certificate is accredited by an entity within the European Union in keeping with a Voluntary Accreditation Structure in accordance with the provisions of Directive 1999/93/EC.
- The certificate is registered in a public register held by a competent signature or tax authority.

In the case of countries outside the European Union if one of the following requirements is met:

- The certificate is accredited by an entity within the European Union in keeping with a Voluntary Accreditation Structure in accordance with the provisions of Directive 1999/93/EC.
- A CA entity within the EU has validated the certificate.
- The certificate is recognized under agreements between the EU and third countries.

6.2. Can electronic invoices be issued from outside Spain on behalf of companies resident in Spain?

The issuing of invoices outside Spanish territory is covered by Article 9 of the Order EHA/962/2007. It is also regulated by Article 5 of Royal Decree 1496/2003 of the Regulations on invoicing obligations.

If the third party, or address in the case of self-invoicing, issuing the invoice is not resident in Spain but is resident in another EU country or country with a legal agreement:

- No es necesaria la autorización previa de la Agencia Tributaria. (Art.5-4 RD 1496/2003).

Si el tercero, o destinatario caso auto factura, que expide facturas no es residente en España, ni en un Estado Miembro de la UE, ni en un país con el que exista un instrumento jurídico:

- Es necesaria la autorización previa de la Agencia Tributaria (Art. 5-4 RD 1496/2003 y Art. 9-3 Orden EHA 962/2007).
- Pueden pedir la autorización a instancias de empresarios o profesionales españoles. No a instancias de residentes en el extranjero, que pretendan homologar sus sistemas para prestar servicios a residentes en España.
- El procedimiento está regulado en el Artículo 9 de la Orden EHA 962/2007.

6.3. ¿En facturación electrónica hay que usar siempre firma electrónica reconocida?

La Orden EHA/962/2007 dice que la obligación de remisión y conservación de facturas o documentos sustitutitos, podrá ser cumplida por medios electrónicos que garanticen la autenticidad del origen y la integridad de su contenido.

Para asegurar tal autenticidad y la integridad se puede:

- Usar firma electrónica reconocida.
- Usar sistemas de intercambio electrónico de datos EDI.

En este caso las partes deben reflejar con precisión los medios empleados para garantizar la autenticidad e integridad.

- Otros sistemas distintos a los anteriores.

En este caso será necesaria una autorización del Director del Departamento de Inspección Financiera y Tributaria.

El escenario más frecuente es usar firma electrónica reconocida.

- No prior authorization is required from the Tax Agency. (Art.5-4 RD 1496/2003).

If the third party, or address in the case of self-invoicing, issuing the invoice is not resident in Spain or in another EU country or country with a legal agreement:

- Prior authorization must be sought from the Tax Agency (Art. 5-4 RD 1496/2003 and Art. 9-3 Order EHA 962/2007).
- Authorization may be sought on behalf of Spanish businesspeople or professionals. Not on behalf of residents abroad wishing to have their systems recognized to provide services to Spanish residents.
- The procedure is regulated in Article 9 of Order EHA 962/2007.

6.3. Must a valid electronic signature always be used on electronic invoices?

Order EHA/962/2007 states that the sending and conservation obligations for invoices and substitute documents may be met by electronic means where said means guarantee the authenticity of origin and integrity of the invoices' content.

To ensure this authenticity and integrity:

- A valid electronic signature or
- An electronic EDI data exchange system may be used.

In this case the parties should precisely state the means used to guarantee authenticity and integrity.

- Systems other than those above.

In this case authorization must be sought from the Director of the Financial and Tax Inspection Department.

The most frequently used system is a valid electronic signature.

Sólo ciertos sectores, en los que lleva tiempo implantando, usan EDI, como por ejemplo el sector de la automoción.

En las preguntas y respuestas aquí expuestas, se sobreentiende que se habla de facturas emitidas con firma electrónica, salvo que se diga expresamente otra cosa.

6.4. Aclaración sobre el alcance legislativo en lo referente a documentos digitalizados

Inicialmente el modelo normativo de digitalización certificada se ha comenzado relacionándolo con aspectos puramente tributarios (facturación). De hecho toda la legislación aplicable a la digitalización certificada únicamente hace referencia a las facturas.

La nueva Directiva sobre e-Facturación indica diferentes medios para recoger la fiabilidad de una factura electrónica:

- Por una parte, sigue contemplando la posibilidad de utilizar la firma electrónica y EDI como sistemas válidos de facturación, opciones que ya se contemplaban en la anterior Directiva.
- Por otra, introduce como novedad la posibilidad de utilizar otros sistemas tecnológicos distintos de los anteriores, como podrían ser: otros tipos de firma electrónica, de EDI, de archivo seguro, intranet, terceras partes de confianza, etc.

Se está preparando una norma española que permita digitalizar, mediante digitalización certificada, también otro tipo de documentos distintos de facturas algo que las empresas llevan tiempo demandando.

Only a limited number of sectors use EDI. These are sectors where this system has been in operation for some time.

All of the questions and answers featured here presume the use of an electronic signature unless otherwise stated.

6.4. Clarification of the legislative scope regarding computerized documents

Initially, the certified computerization regulation model only covered tax-related issued (invoicing). In fact, all of the legislation applicable to certified computerization only makes reference to invoices.

The new Directive on e-Invoicing sets out a range of measures to recognize the reliability of an electronic invoice:

- It continues to provide the possibility of using an electronic signature and EDI as valid invoicing systems. These options were included in the previous Directive.
- It also establishes the possibility of using technological systems other than those mentioned above, such as: other types of electronic signature, EDI, secure files, intranet, trusted third parties, etc.

Spanish regulations are been drawn up permitting the computerization, by means of certified computerization, of other sorts of documents beyond invoices. Business has been asking for this option for some time.

Switzerland

Author:

Marc Philipp Gugger
Rechtsanwalt

Ernst & Young AG, Legal Services,
Belpstrasse 23, Postfach, CH-3001 Bern

E-Mail: marc.gugger@ch.ey.com

Telefon: +41 58 286 61 90

Internet: http://www.ey.com/ch

1. Rechtliche Rahmen- bedingungen unter Berücksichtigung des Steuerrechts

1.1. Vorbemerkungen

Eine nicht gesetzeskonforme Archivierung von Geschäftsunterlagen kann zu Rechtsnachteilen und zum Verlust von Beweismitteln führen und so bei rechtlichen Auseinandersetzungen kostspielige Folgen nach sich ziehen. Insbesondere im Bereich der Mehrwertsteuer kann eine Kontrolle laut Art. 49 des Bundesgesetzes über die Mehrwertsteuer (MWSTG) zu einer Aufrechnung bzw. Steuernachforderung über die letzten fünf Jahre führen. Deshalb ist es wichtig, dass bei der Einführung eines elektronischen Aufbewahrungssystems die einschlägigen Bestimmungen eingehalten werden.

1.2. Grundlagen

Es gilt sowohl die allgemeinen handels-rechtlichen, als auch die spezifischen steuerrechtlichen Bestimmungen zu beachten, so insbesondere:

- Das Schweizerische Obligationenrecht (OR);
- Die Verordnung des Bundesrates über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV);

1. General legal conditions including tax laws

1.1. Preamble

Archiving of business documents in disregard of statutory provisions can have legal repercussions and result in a loss of evidence, thereby proving costly during legal disputes. Especially as regards value added tax, an audit of such tax as per Art. 49 of the Federal Value Added Tax Act can lead to offset claims or additional demands spanning the last five years. For this reason, it is important to observe relevant regulations when implementing an electronic safekeeping system.

1.2. Principles

Besides the provisions laid down by commercial law, specific provisions of tax laws apply, in particular:

- the Swiss Code of Obligations (OR);
- the Federal Council's decree on maintaining and storing account books (GeBüV);

- Die Verordnung zum MWSTG (MWSTGV);
- Die Verordnung über elektronische Daten und Informationen (ElDI-V);
- Das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES).

1.3. Aufbewahrungsfristen

Geschäftsbücher, Buchungsbelege sowie Geschäftskorrespondenz sind nach Art. 962 OR grundsätzlich 10 Jahre lang aufzubewahren. Namentlich im Mehrwertsteuerrecht gelten teilweise längere Aufbewahrungsfristen.

Die Aufbewahrungsfrist von mehrwertsteuerrelevanten Belegen richtet sich nach der Verjährungsfrist der betreffenden Steuerforderung. Mehrwertsteuer-Forderungen verjähren laut Art. 49 Abs. 1 des MWST nach 5 Jahren, absolut nach 15 Jahren und entsprechend lang sind die Belege aufzubewahren. Die mit Immobilien zusammenhängenden Geschäftsunterlagen hingegen sind gemäss Art. 58 Abs. 2 MWSTG während 20 Jahren aufzubewahren, in Spezialfällen sogar bis zu 25 Jahre.

In der Praxis empfiehlt sich, bei der Archivierung von Dokumenten die relevanten Aufbewahrungsfristen zu ermitteln und die Dokumente in entsprechende Kategorien einzuteilen sowie aufzubewahren.

1.4. Aufbewahrungsform

Nach Art. 957 OR können die Bücher, die Buchungsbelege und die Geschäftskorrespondenz auch elektronisch oder vergleichbarer Weise geführt und aufbewahrt werden, soweit dadurch die gesetzlichen Vorschriften eingehalten werden; Betriebsrechnung und Bilanz hingegen sind in jedem Fall schriftlich, d.h. in Papierform und mit Originalunterschrift, aufzubewahren.

- the ordinance on value added tax (MWSTGV);
- The ordinance on electronic data and information (ElDI-V);
- The federal law regarding certification services for electronic signatures (ZertES).

1.3. Safekeeping periods

Art. 962 of the Obligations Act specifies a basic safekeeping period of 10 years for account books, accounting records and business correspondence. Longer safekeeping periods sometimes apply under laws applicable to sales tax.

The safekeeping period for records of relevance to value added tax depends on the statutory period of limitation for the tax demands under consideration. According to Art. 49 Sec. 1 of value added tax laws, claims for value added tax expire under the statute of limitations after 5 years, and absolutely after 15 years; the safekeeping period for relevant records is correspondingly long. According to Art. 58 Sec. 2 of value added tax laws, business documents related to real estate are to be stored for 20 years, even 25 years in special cases.

In practice, it is advisable to ascertain safekeeping periods applicable to documents intended for storage and classify these documents appropriately by their respective safekeeping periods.

1.4. Safekeeping form

According to Art. 957 of the Obligations Act, books, accounting records and business correspondence can also be maintained in electronic or similar form provided that relevant legislation is adhered to; however, operating accounts and balance sheets must be stored in writing, i.e. on paper with original signatures.

1.5. Aufbewahrungsort

Bei international tätigen Firmen kann es sinnvoll sein, sämtliche Geschäftsbücher und Belege konsolidiert im Ausland aufzubewahren. Bis Ende 2009 war dies jedoch gemäss der Wegleitung 2008 zur Mehrwertsteuer der Eidgenössischen Steuerverwaltung (ESTV) ausdrücklich verboten. Heute fehlt zwar eine entsprechende Weisung, dennoch hält die ESTV weiterhin an dieser Praxis fest, wonach Geschäftsbücher und Belege grundsätzlich zwingend physisch im Inland, also in der Schweiz, aufzubewahren sind. Weiterhin unklar bleibt allerdings, ob diese Pflicht auch für die rein elektronische Archivierung gelten kann, was unseres Erachtens eher zu verneinen ist. In jedem Fall sind aber, auch bei der elektronischen Aufbewahrung im Ausland, sämtliche rechtlichen Rahmenbedingungen einzuhalten und insbesondere der Zugriff, die Lesbarmachung und Auswertung der für die Steuererhebung relevanten Daten jederzeit zu gewährleisten (vgl. Art. 10 Abs. 4 EIDI-V).

1.5. Safekeeping place

It can be sensible for internationally active companies to keep all accounting records together in one place abroad. Up to the end of 2009, however, this was expressly forbidden in accordance with the 2008 Guidance on VAT issued by the Swiss Federal Tax Administration (ESTV). Although today there is no such advice, the Swiss Federal Tax Administration continues to hold to this practice according to which account books and accounting records must mandatorily be kept physically domestically, i.e. in Switzerland. However, it remains unclear as to whether this obligation can also apply to archiving by purely electronic means, which in our view ought to be answered in the negative. In any event, however, even in the case of electronic safekeeping abroad, all legal conditions must be observed and in particular access, readability and analysis of the data relevant for fiscal purposes have to be safeguarded at all times (cf. Art. 10 Sec. 4 EIDI-V).

1.6. E-Mails und elektronische Rechnungen

Die elektronische Rechnungsstellung ist in der Schweiz seit Inkrafttreten der ElDI-V möglich. Die ElDI-V regelt die technischen, organisatorischen sowie verfahrenstechnischen Anforderungen an Beweiskraft und Kontrolle von elektronisch oder in vergleichbarer Weise übermittelten und aufbewahrten Daten und Informationen. Betroffen sind davon namentlich all jene Dokumente, die für den Vorsteuerabzug, die Steuererhebung oder den Steuerbezug relevant sind, wie elektronische Rechnungen. Verlangt wird insbesondere eine fortgeschrittene elektronische Signatur, welche auf einem Zertifikat beruht, das von einem gemäss ZertES anerkannten Zertifizierungsdiensteanbieter stammt. Im Rahmen der Verwendung der digitalen Signatur müssen die Teilnehmer im Rechnungsbearbeitungsprozess verschiedene Handlungen vornehmen, damit die elektronisch übermittelten Rechnungen als beweiskräftig anerkannt werden.

1.6. E-mails and electronic invoices

Electronic invoicing has been permissible in Switzerland since coming into effect of ElDI-V (ordinance on electronic data and information). This ordinance specifies technical, organizational and procedural requirements for validating and verifying data and information communicated and stored electronically or using similar means. Concerned here are all documents of relevance to input tax deduction, tax determination and tax collection, as well as electronic invoices. Required here, in particular, is an advanced, electronic signature based on a certificate originating from a certification service provider approved according to ZertES. Participants employing digital signatures must follow a set of instructions during the invoicing process in order for the electronically submitted invoices to have a conclusive status.

So müssen unter anderem die Daten nach der abgeschlossenen Übermittlung, spätestens vor ihrer Verwendung mittels Verifikation der digitalen Signatur auf Integrität, Authentizität und Signaturberechtigung überprüft werden. Das Verifikationsergebnis ist zu dokumentieren. Der zur Überprüfung erforderliche öffentliche Schlüssel muss zusammen mit den abgesicherten Daten aufbewahrt werden.

In diesem Zusammenhang ist zu beachten, dass die blosse Übermittlung einer PDF-Datei als Anhang eines E-Mails diesen Anforderungen nicht zu genügen vermag.

1.7. Anforderungen an die elektronische Archivierung

Die Anforderungen zur elektronischen Archivierung finden sich in der GeBüV. Bei elektronisch übermittelten Dokumenten sind im Zusammenhang mit der Mehrwertsteuer zusätzlich die MWSTGV sowie die ElDI-V zu beachten. Nach Art. 3 GeBüV müssen die Geschäftsbücher so geführt und aufbewahrt und die Buchungsbelege und die Geschäftskorrespondenz so erfasst und aufbewahrt werden, dass sie nicht geändert werden können, ohne dass sich dies feststellen lässt.

Je nach Art und Umfang des Geschäfts sind laut Art. 4 GeBüV die Organisation, die Zuständigkeiten, die Abläufe und Verfahren und die Infrastruktur (Maschinen und Programme), die bei der Führung und Aufbewahrung der Geschäftsbücher zur Anwendung gekommen sind, in Arbeitsanweisungen so zu dokumentieren, dass die Geschäftsbücher, die Buchungsbelege und die Geschäftskorrespondenz verstanden werden können; Arbeitsanweisungen sind zu aktualisieren und nach den gleichen Grundsätzen und gleich lang aufzubewahren wie die Geschäftsbücher, die danach geführt wurden.

Prior to a use of data whose transmission has been completed, for instance, it is necessary to check the data's integrity, authenticity and signature qualification by verifying the digital signature. The results of the verification process must be documented. The public key required for checking must be saved together with the backed-up data.

In this context, it is necessary to note that mere transmission of a PDF file as an e-mail attachment does not prove sufficient to fulfill these conditions.

1.7. Requirements for electronic archiving

Electronic archiving requirements are laid down by the Federal Council's decree on maintaining and storing account books (GeBüV). In the case of electronically transmitted documents of relevance to value added tax, it is also necessary to observe the ordinances on value added tax (MWSTGV) as well as electronic data and information (ElDI-V). According to Art. 3 of GeBüV, maintenance and storage of account books as well as registration and storage of vouchers and business correspondence are to be performed in a manner ensuring that manipulations to them will not go unnoticed.

Depending on the nature and scope of the business, Art. 4 of GeBüV specifies that the organization, responsibilities, workflows, procedures and infrastructure (machines and programs) involved in maintenance and safekeeping of account books are to be documented in work instructions such that the account books, accounting and business correspondence are comprehensible; the work instructions should be updated as required and stored for the same periods according to the same principles applicable to the related account books.

Die Geschäftsbücher, die Buchungsbelege und die Geschäftskorrespondenz müssen so aufbewahrt werden, dass sie bis zum Ende der Aufbewahrungsfrist von einer berechtigten Person innert angemessener Frist eingesehen und geprüft werden können; soweit es für die Einsicht und die Prüfung erforderlich ist, sind das entsprechende Personal sowie die Geräte oder Hilfsmittel gemäss Art. 6 GeBüV verfügbar zu halten.

Die Informationen sind nach Art. 8 GeBüV systematisch zu inventarisieren und vor unbefugtem Zugriff zu schützen; Zugriffe und Zutritte sind aufzuzeichnen, wobei diese Aufzeichnungen derselben Aufbewahrungspflicht wie die Datenträger unterliegen. In diesem Zusammenhang ist zu beachten, dass auch sämtliche Lesezugriffe auf das Archiv aufzuzeichnen sind. Es sind zudem gemäss Art. 10 Abs. 1 GeBüV regelmässige, stichprobenweise Kontrollen der Datenlesbarkeit durchzuführen und bei ersten Anzeichen einer zukünftig eingeschränkten Lesbarkeit ist eine Datenmigration auf neue Medien vorzunehmen.

Wir empfehlen, bei der Einführung eines elektronischen Archivierungssystems vorgängig genau abzuklären, welche Anforderungen (und Aufbewahrungsfristen) zu beachten sind und wie deren Einhaltung sichergestellt werden kann. Insbesondere die lückenlose Aufzeichnung sämtlicher Lesezugriffe auf archivierte Unterlagen ist sicherzustellen. Zudem hat es sich in der Praxis bewährt, das System als Ganzes durch einen (externen) Experten vor der Inbetriebnahme in technischer und juristischer Hinsicht überprüfen zu lassen.

Account books, accounting records and business correspondence must be stored such that they can be viewed and inspected by authorized persons at reasonably short notice until the end of the stipulated storage period; as per Art. 6 of GeBüV, staff as well as equipment and aids are to be provided to the extent required for viewing and examining the documents.

Information is to be inventoried systematically and protected against unauthorized access as per Art. 8 of GeBüV; access and viewing operations are to be logged, the logs being subject to the same safekeeping obligations as the data carriers. In this regard, it is necessary to note that all operations obtaining read access to the archive must be logged as well. Moreover, as per Art. 10 Sec. 1 of GeBüV, regular, spot checks of data readability are to be performed; on the first sign of any impending impairment to readability, the data are to be migrated to new media.

Before an electronic archiving system is implemented, we recommend precisely determining which requirements (and safekeeping periods) apply and how adherence to them can be ensured. To be ensured, in particular, is complete logging of all operations obtaining read access to archived documents. Moreover, having the entire system inspected from the technical and legal standpoints by an (external) expert prior to commissioning is a measure which has proven itself in practice.

2. Beweiskraft

2.1. Zulässige Beweismittel

Art. 957 Abs. 4 OR hält explizit fest, dass elektronisch oder in vergleichbarer Weise aufbewahrte Geschäftsbücher, Buchungsbelege und Geschäftskorrespondenz die gleiche Beweiskraft haben wie Originale resp. solche, die ohne Hilfsmittel lesbar sind.

2. Probative force

2.1. Permissible items of evidence

Art. no. 957 Sec. 4 of the Swiss Code of Obligations explicitly states that account books, accounting records and business correspondence stored electronically or in similar form have the same probative force as original documents or those which can be read without any aids.

Hierbei handelt es sich um eine zwingende Beweisregel des Bundesrechts, die durch die besonderen Vorschriften über die Aufbewahrung derartiger Dokumente gerechtfertigt wird. In Bezug auf Beweiskraft der genannten Geschäftsdokumente besteht somit grundsätzlich kein Unterschied zwischen schriftlich oder elektronisch aufbewahrten Dokumenten. Vor Gericht werden sowohl nicht unterzeichnete Dokumente (d. h. also z. B. auch Ausdrucke elektronischer Dokumente von Computern oder Scans) als auch Kopien von unterzeichneten Dokumenten zum Beweis zugelassen.

This mandatory federal law on evidence is justified by the special regulations concerning safekeeping of such documents. In principle, there is therefore no difference between storage in written or electronic form when it comes to the probative force of the above-mentioned business documents. Unsigned documents (including computer printouts of electronic documents and scans) as well as copies of signed documents are permissible as items of documentary evidence before courts.

Bei der elektronischen Aufbewahrung von ursprünglich in Papierform ausgestellten und verschickten Rechnungen ist daher die Vernichtung der Originalbelege gemäss den erläuterten Vorschriften grundsätzlich möglich und zulässig. In der Praxis besteht jedoch die Gefahr, dass dem Beweispflichtigen in einem Prozess vor Gericht daraus unter Umständen Nachteile entstehen können. Denn es bleibt selbstverständlich das allgemein geltende Prinzip der freien Beweiswürdigung durch den Richter. Im Prozessfall kann nämlich mit der vorerwähnten Bestimmung keine absolute Gleichstellung von Aufzeichnung und Original herbeigeführt werden. Wenn jemand ein Dokument vorlegt und im Streitfall dessen Echtheit zu beweisen hat, dann ist davon auszugehen, dass ihm dies bei Vorweisung des Originals einer handgeschriebenen Schuldanerkennung respektive eines E-Mails mit einer elektronischen Signatur leichter gelingen wird als bei Vorlage einer Aufzeichnung oder eines Ausdrucks. Dabei sind jedoch stets die Besonderheiten des einzelnen Falles massgeblich.

In the case of electronically stored invoices initially prepared and issued on paper, the original documents therefore can and may be destroyed according to the mentioned regulations. In practice, however, there is the risk that there coould be disadvantages arising from this under certain circumstances for the person obliged to furnish proof in a court case. The generally applicable principle of independent assessment of evidence at the judge's discretion by all means naturally remains in effect. In the event of litigation, the afore-mentioned provision does not ensure absolute equivalence between a record and its original. If a submitted document's authenticity needs to be demonstrated in the event of a legal dispute, this might be achieved more easily, for example, by presenting an original, hand-written debt instrument or electronically signed e-mail, rather than presenting a record or printout. Special circumstances pertaining to each individual case nonetheless prove ultimately authoritative.

2.2. Besonderheiten im Strafrecht

Zusätzlich zu der vorerwähnten freien Beweiswürdigung tritt im Strafrecht der Grundsatz „Im Zweifel für den Angeklagten“. Im Zweifellsfall hat daher der Richter in Sachverhaltsfragen von der Version auszugehen, die günstiger ist für den Angeklagten.

2.2. Special aspects related to criminal law

Besides prescribing the afore-mentioned, independent assessment of evidence, criminal law gives the accused party the benefit of the doubt in case of uncertainty. In such cases, the judge must therefore go by the version more favorable for the accused party when taking circumstances into consideration.

2.3. Besonderheiten bei E-Mails und elektronischen Rechnungen

Wie unter Ziffer 2.1 dargelegt, kann aufgrund des Prinzips der freien Beweiswürdigung durch den Richter nicht ausgeschlossen werden, dass im Streitfall ein handschriftliches Original oder ein E-Mail mit einer elektronischen Signatur gemäss ZertES höher gewichtet wird als ein simpler Ausdruck. Mit einer elektronischen Signatur können nämlich sowohl der Inhalt einer Mitteilung als auch die Zuordnung zu einer bestimmten Person eindeutig nachgewiesen werden.

2.3. Special aspects related to e-mails and electronic invoices

As mentioned under item 2.1, the principle of independent assessment of evidence by judges does not rule out that a handwritten, original document or e-mail with an electronic signature according to ZertES will carry more weight than a simple printout in the event of a dispute. An electronic signature definitively verifies a message's contents as well as the person who issued the message.

2.4. Beweislast des Zuganges von E-Mails

Der Zugang ist nach allgemeinen prozessualen Grundsätzen vom Versender zu beweisen. Bei Schriftstücken erfolgt dies durch zwei Teilbeweise, indem einerseits das Eintreffen bewiesen wird, beispielsweise durch eine Empfangsbestätigung, und andererseits die Verfassung der Erklärung, beispielsweise durch die Vorlage einer Briefkopie. Beide Teilbeweise zusammen erbringen den Zugangsbeweis. Bei E-Mails kann häufig eine Antwort-E-Mail des Empfängers, welche die empfangene Nachricht zitiert, diese Funktion übernehmen.

Es besteht die herrschende Lehrmeinung, dass bei E-Mails die Zustellung allgemein als erfolgt gilt, wenn die Mitteilung auf dem Server des Empfängers gespeichert wird. Dies jedoch nur unter der Voraussetzung, dass mit Kenntnisnahme zu rechnen ist. Letzteres ist insbesondere dann nicht der Fall, wenn die Zustellung an eine private E-Mailadresse erfolgt, welche dem Versender nicht ausdrücklich mitgeteilt wurde.

2.4. Burden of proof regarding receipt of e-mails

Receipt is to be proven by the sender in accordance with general procedural principles. In the case of documents, this is done by means of two items of partial evidence; firstly by proving delivery, e.g. through confirmation of receipt, and secondly by preparing a statement, e.g. involving presentation of a copy of the letter. Both items of partial evidence together serve to prove that the document was received. In the case of e-mails, this function can often be performed by a response mail issued by the recipient and specifying the message received.

According to the prevalent school of thought, an e-mail is generally considered delivered once it has been saved on the recipient's server. However, this only applies provided that an acknowledgement can be expected. This is not always the case, especially if the e-mail is delivered to a private address which was not indicated explicitly to the sender.

Exkurs: Einzig in der kürzlich erlassenen „Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens“, welche alleine auf Verfahren vor Bundesbehörden Anwendung findet, wird diese Frage klar geregelt. Stellt die Behörde der Adressatin oder dem Adressaten den Versand in einem elektronischen Postfach zur Verfügung, so gilt in diesem Fall, entgegen der oben genannten Lehrmeinung, der Zeitpunkt des Herunterladens als Zeitpunkt der Zustellung gemäss Art. 10 Abs. 1 dieser Verordnung.

Note: This issue is only clearly settled by the recently enacted ordinance on electronic communications as part of administrative proceedings applicable to hearings before federal authorities. If an authority sends an e-mail to an addressee, contrary to the school of thought mentioned above, the moment of downloading from the electronic mailbox counts as the time of delivery as per Art. 10 Sec. of this ordinance.

In der Praxis werden E-Mails häufig umgehend beantwortet, wobei das E-Mail-Programm standardmässig die ursprüngliche Nachricht zitiert. Dadurch kann immerhin der Zugang (mit einer elektronischen Signatur auch der Inhalt) des E-Mails durch Vorlage des gesamten Mailverkehrs einfach bewiesen werden.

In practice, e-mails are usually answered promptly, the e-mail software citing the original message by default. Consequently, receipt of an e-mail can be easily proven by presenting the entire thread of communications.

Exkurs: Schliesslich bleibt die Konstellation bestehen, dass jemand eine E-Mail fälscht und behauptet, diese sei ihm vom fiktiven Versender zugestellt worden. Sofern Letzterer aber eine elektronische Signatur gemäss ZertES verwendet, kann er sich auch hier erfolgreich gegen den Vorwurf wehren, da die Signatur bei der Fälschung fehlen wird.

Note: Finally, there is the possibility that someone might forge an e-mail and fictitiously claim that it was sent to them by a fictitious sender. If the latter uses electronic signatures in compliance with ZertES, he can successfully defend themselves against this accusation because the forged e-mail would lack such a signature.

2.5. Aufbewahrung von E-Mails

Für die Aufbewahrung von E-Mails existieren keine Sondervorschriften, so dass die oben dargelegten Bestimmungen nach Art. 957 OR sowie der GeBüV zur Anwendung kommen, insofern die E-Mails zur Korrespondenz oder den Belegen gehören. Dementsprechend kann auf die in diesem Zusammenhang in Ziffer 1.5 und 1.6 gemachten Ausführungen verwiesen werden.

2.5. Safekeeping of e-mails

Because safekeeping of e-mails is not governed by any special regulations, the above-mentioned provisions of Art. 957 of the Obligations Act and the decree on storing and maintaining account books apply to e-mails forming part of correspondence and accounting records. Accordingly, reference can be made to the related statements under items 1.5 and 1.6.

United Kingdom

Author:

Alan Shipman
Managing Director

Group 5 Training Limited

e-mail: a.shipman@group5.co.uk

www.group5.co.uk

1. Fiscal aspects

1.1. Storage format

The issues related to the requirements for the storage of documents on paper or in an electronic form on appropriate storage media (or on microfilm) have been debated for many years. The debate continues!

In general terms, UK legislation does not state the format or media used for the storage of information. Research on this topic has not identified any specific legislation that requires (in particular) paper based document. However, there are many requirements related to the various industry regulators that require, mainly for historic reasons, paper based original documents to be retained, most frequently with an original handwritten signature or a seal. This situation is changing, with many regulators now accepting well managed electronic creation and storage of corporate records as normal practice.

In United Kingdom government terms, HM Revenue and Customs (HMRC), whose role is to "*make sure that the money is available to fund the UK's public services [and] helps families and individuals with targeted financial support*" is strongly promoting electronic interaction and submission of information. Full details of their services are available at http://www.hmrc.gov.uk/index.htm. In practice, they offer little specific guidance on storage format. In October 1998, they did offer some advice in an article related to the keeping of records under Self Assessment corporation tax rules[1]. This article included the following statement:

"*We accept of course that companies which store information in accordance with the Code of Practice on the Legal Admissibility of Information stored in Electronic Document Management Systems (BSI 1996 DISC PD 0008[2]) will thereby automatically satisfy the tax requirements.*"

[1] http://www.hmrc.gov.uk/ctsa/ctsaguide.pdf

[2] DISC PD 0008 was a predecessor to and is superseded by BS 10008:2008

1.2. Retention periods

Within the UK, there are many pieces of legislation and regulation that give document retention period requirements. One such piece of legislation that is widely referenced is the Limitations Act 1980[3] which applies to England and Wales. There are similar rules in Northern Ireland, and other (different) rules in Scotland. The E&W Limitations Act lists many types of documents and puts 1, 2, 3, 6, 12 or unlimited retention period requirements on them. Perhaps the most important of these is the 6 years retention related to claims for breaches of contract (12 years where the contract was executed as a deed).

For financial records, various legislations such as the Companies Act 1985 and the VAT Act 1994 state minimum legal retention periods – typically they are 6 years from the end of the current financial year.

The whole issue of legal retention periods within the UK is complex and sometimes contradictory. There are a number of publications which identify some retention requirements; a useful and up to date list of a significant range of these can be found in "The ICSA Guide to Document Retention"[4]. This regularly updated publication details the retention requirements for most general types of document, including those related to Companies law, meetings and minutes, accounting and tax records, employment and pension records, health and safety, contracts and property records and financial services records.

There is also legislation related to the retention of personal information. The 5th Principle of the Data Protection Act 1998 requires that personal information is retained 'for no longer than is necessary'. Such a requirement is another reason why formal retention policies and schedules are essential for all organisations.

Some of the required retention periods are very long, often decades, which raises other issues that should be considered as part of a properly defined retention policy. Will the electronic media still be readable and will the electronic format be accessible when the electronic document is needed? It is important that authenticity and integrity of the information is not compromised by media migrations or format conversions.

1.3. E-mails

Within UK legislation, an e-mail is a document, and can (depending upon its content) be an organisational record. The fact that the document is an e-mail (or an attachment to an e-mail) is of no particular relevance.

[3] http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1980/cukpga_19800058_en_1

[4] Andrew C. Hamer, 2nd edition published in 2008 by the Institute of Chartered Secretaries and Administrators, see http://www.icsabookshop.co.uk/disp.php?ID=633

E-mail is normally considered as legally admissible within UK courts. In order to ensure that sufficient evidential weight is afforded to e-mails, the electronic systems which manage them must be reliable and must have sufficiently robust audit trails in order to provide evidence of this reliability. A section of BIP 0008-2:2008[5] deals specifically with the management of e-mail systems. Where proof of electronic identity is important, then BIP 0008-3:2008[6] gives good practice advice.

1.4. Electronic invoices

HMRC issued guidance on electronic invoicing in June 2007[7]. This guidance is aimed at the issuing, receiving and storing of VAT invoices in an electronic format.

The guidance comments that "the law does not compel you to use electronic invoicing. It's up to you whether you issue paper or electronic VAT invoices". There is also no requirement (since January 2006) to notify the HMRC that electronic VAT invoicing will be used.

There is additional advice about "dual systems" (e.g. both paper and electronic); these are only allowed during controlled trials of the electronic system. Once the trials are complete, the electronic VAT invoice is the "legal document".

Importantly, the guidance stresses authenticity and integrity of the electronic invoice by commenting that "you may invoice electronically where the authenticity of the origin and integrity of the invoice data are guaranteed". The guidance then identifies "advanced electronic signatures", "EDI" or "other means" as a way of achieving the required guarantee.

1.5. Destruction of original documents

Another discussion on storage formats that has taken place in the UK has been the legal position with the destruction of original documents once they have been scanned. Again, no formalised conclusion has been reached on this issue, but many organisations have taken the decision following a risk assessment and are destroying paper originals based on the low risks involved and the (often) significant enhancements to business processes achievable. An important factor that will feature in the risk assessment and resulting policies and procedures, where the decision to destroy paper originals is taken, is the timing of the destruction relative to the scanning processes.

[5] BIP 0008-2:2008 Evidential weight and legal admissibility of information transferred electronically, published by the British Standards Institution

[6] BIP 0008-3:2008 Evidential weight and legal admissibility of linking electronic identity to documents, published by the British Standards Institution

[7] http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageVAT_ShowContent&id=HMCE_PROD_010205&propertyType=document

For many years, UK organisations have been scanning original documents and storing the resultant images on microfilm of various formats. Such a process has rarely been challenged in court. Where evidential weight is important, microfilming processes compliant with BS 6498:2002 *Guide to the preparation of microfilm and other microforms that may be required as evidence* have been used to resist legal challenges. The equivalent for electronic scanning and storage processes is BS 10008:2008 *Evidential weight and legal admissibility of electronic information - Specification*. BIP 0008-1:2004[8] has been submitted to ISO and is now published as ISO 15801:2009 *Information stored electronically, recommendations for trustworthiness and reliability*.

In all cases where original document have (or have not) been destroyed after microfilming / scanning, the 'best evidence' rule may be used. This rule talks about the fact that evidence may not be admitted in court if it is not "the best that the nature of the case will allow". This translates, in document management terms, to the fact that the best evidence is always the original document. However, if it can be shown that the original document does not exist, then an authentic copy of the original will be the best evidence. In practice, all relevant evidence is admitted, whether it is an original or a copy. The goodness or badness of the evidence goes only to weight, and not to admissibility.

2. Civil law aspects

2.1. Force of evidence of electronic documents in comparison

In a UK court, legal admissibility is the ability for documents to be accepted as evidence in a particular case. Evidential weight relates to the ability to demonstrate the authenticity and integrity of these documents. Neither should be confused with evidential value of the particular documents.

In the vast majority of cases, possibly in all cases because there are no recognised precedents on this issue, legal admissibility is not an issue. There are specific exclusions from admissibility in criminal law cases related to specific types of information, but these exclusions do not relate to the format (e.g. paper or electronic) of the documents. Evidential weight can be an issue, particularly where the opposing party in litigation challenges the authenticity or integrity of a submitted document.

The UK Civil Evidence Act 1995 contains the following statements related to copies of originals and evidence (see Sections 8 and 9):

[8] BIP 0008-1:2008 Evidential weight and legal admissibility of information stored electronically, published by the British Standards Institution

Proof of statements contained in documents

(1) *Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved:*
(a) by the production of that document, or
(b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such a manner as the court may approve.

(2) It is immaterial for this purpose how many removes there are between a copy and the original.

Proof of records of business or public authority

(1) *A document which is shown to form part of the records of a business or public authority may be received in evidence in civil proceedings without further proof.*

(2) A document shall be taken to form part of the records of a business or public authority if there is produced to the court a certificate to that effect signed by an officer of the business or authority to which the records belong.

Based on these rules and guidelines, many organisations within the UK have taken the decision to destroy some of their original documents, or not create paper based documents in the first place. On the other hand, there are many organisations who consider the risks related to the destruction of original document too high to take this decision.

All members of the legal profession are now required to consider digital evidence but few regard it as their core competency. They often refer to the specialists or specialist treatises in this area, some of which are referenced at the link below [9].

2.2. Special characteristics of e-mail

As noted above, there are no special legal issues related to e-mail within UK legislation. An e-mail is treated as a document / record in the same way as a document in any other format. Similarly, telex transmissions, faxes and SMS / IM messages are treated as documents by the courts.

The issue of the legal admissibility of electronic signatures has been addressed by UK legislation. The Electronic Communications Act 2000[10] defines an 'electronic signature' and states that an electronic signature is admissible as evidence in court.

In addition, UK law incorporates the Electronic Signatures Regulations 2002[11], which defines an 'advanced electronic signature' and a 'certificate'. These regulations were in response to the EC Directive 1999/93/EC on a Community framework for electronic signatures, and relate to the supervision of electronic signature certification service providers.

[9] http://www.stephenmason.eu/books/

[10] http://www.opsi.gov.uk/acts/acts2000/ukpga_20000007_en_1

[11] http://www.opsi.gov.uk/SI/si2002/20020318.htm

2.3. Burden of proof of access

When documentary evidence in any form is challenged in court, then there is a burden of proof on both parties. The challenger will need to disprove, or at least cast significant doubt on the evidence and the submitter will need to demonstrate that it is authentic and that its integrity has not been compromised.

Thus, when managing electronic documents in a document management system, proof (typically by the demonstration of good, documented process and technology and by the provision of authenticated audit trail information) of creation, capture and storage may be crucial in resisting a legal challenge.

Within the UK, such proof is best achieved by following what is considered as best practice. This best practice is documented in BS 10008:2008 *Evidential weight and legal admissibility of information stored electronically* (see above).

This British Standard has been published in the format of a 'Management System Standard', as used in ISO publications such as ISO 9000 (Quality Management) and ISO 27001 (Information Security Management). These International Standards use the "Plan – Do – Check – Act" cycle, resulting in the application of the establishing, implementing, operating, monitoring, exercising, maintaining and improving the effectiveness of the system under consideration. By using this cycle, the management of documents by an organisation in a way that enables the burden of proof to be confidently managed can be incorporated within the overall information management strategy.

2.4. Avoiding liability

There a few legal penalties for breaching corporate retention schedules. One of the relevant pieces of legislation here is the Data Protection Act 1998, under which an individual can require to have their personal information deleted if it is retained for longer than is necessary (see above).

There are penalties for the destruction of documents where they are involved (or potentially involved) in legal proceedings[12]. Such destruction can be deemed as contempt of court (e.g. the improper interference with the administration of justice). Such contempt can lead to fines and/or imprisonment under UK legislation.

There are, however, many business reasons why the non-implementation of retention schedules can lead to the need for additional administrative resource. For example, under the Freedom of Information Act 2000[13] (or the similar FOI (Scotland) Act 2002), if information is held, even if is past its retention period, then it may need to be located and disclosed when it is the subject of a legal request for information under the Act. The same is true in relation to a subject access request made under the Data Protection Act 1998.

[12] 'Proceedings' here includes the responding to a subject access request under the DPA

[13] http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

There are many other 'non-legal' benefits in compliance with retention schedules. These include the reduction in storage and management costs. Where electronic documents are involved, compliance with retention schedules can lead to the avoidance of the need to convert electronic documents to new software formats (to ensure continued access to the information contained in the document by the replacement of old – no longer supported – software formats), or a reduction in the resources necessary when migrating electronic documents to new electronic storage media.

Disclaimer

The information provided above is without engagement and is intended solely to provide you with a general overview of the problems without any pretension to completeness or accuracy of detail. This Statement is not designed to clarify the details of individual legal regulations or all aspects of the subjects addressed and does not replace legal and tax advice in individual cases. Before making any business decisions you should consult your tax adviser, auditor or attorney. The legal regulations may have changed since this text was published.

Über das Competence Center Steuern und Recht (CCSR)

Das Competence Center „Steuern und Recht“ beschäftigt sich mit allen steuerlichen und rechtlichen Fragestellungen im Umfeld elektronischen Archivierung, Dokumenten-management und Enterprise Content Management.

Die wichtigsten Bereiche sind hierbei:

- Steuerrechtliche Vorgaben, insbesondere die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlangen (GDPdU) und Umsatzsteuer
- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)
- Handelsrechtliche Vorgaben
- Privatrechtliche Vorgaben
- Datenschutzrechtliche Aspekte
- Rechtssicherer Einsatz von digitalen Signaturen
- Branchespezifika (Pharma, Automotive, Behörden)
- Sonstige DMS-bezogene regulatorische Anforderungen

Typische Themen in den obigen Bereichen sind:

- Archivierung von papierbasierten Eingangs- und Ausgangsdokumenten
- Archivierung von elektronischen Eingangs- und Ausgangsdokumenten
- Archivierung von Dokumenten mit elektronischer Signatur
- Archivierung von EMails
- Archivierung von steuerrelevanten Daten
- Revisionssicherheit (Nachvollziehbarkeit, Dokumentation, Vollständigkeit, Unveränderbarkeit)
- Löschpflichten von personenbezogenen Daten und Dokumenten

The Competence Center Taxation and Law (CCSR)

The Competence Center "Taxation and Law" deals with all taxation and legal issues relating to electronic archiving, document management and enterprise content management.

The main areas are:

- Tax regulations, in particular the principles of data access and verifiability of digital documents (GDPdU) and VAT
- Principles of correct computer-based accounting systems (GoBS)
- Commercial law
- Private law
- Data protection issues
- Digital signatures
- Industry-specific rules (pharmaceutical, automotive, government)
- Other DMS-related regulatory requirements

Typical issues in the above areas are:

- Archiving paper-based incoming and outgoing documents
- Archiving electronic incoming and outgoing documents
- Archiving documents with electronic signatures
- Archiving emails
- Archiving tax-relevant data
- Audit compliance (traceability, documentation, integrity, immutability)
- Obligations to delete personal data and documents

- Inhalte einer Verfahrensdokumentation
- Verwaltung von Aufbewahrungsfristen
- Praktische Umsetzung von regulatorischen Anforderungen

Das CC „Steuern und Recht“ ist die verbandsinterne Anlaufstelle für alle DMS-bezogenen rechtlichen Fragestellungen. Zielsetzung ist der Wissenstransfer zu den Mitgliedern, Verbesserung der Meinungs-bildung und Schaffung von Defacto-Standards. Die Besetzung mit Anbietervertretern, Beratern, Wirtschaftsprüfern und Rechtsanwälten soll eine ganzheitliche Sichtweise sicherstellen.

Durch Veröffentlichungen, Stellungnahmen, Fachtagungen, Roadshows und die gezielte Beantwortung von individuellen Fragestellungen sollen die VOI-Mitglieder und Interessenten bezüglich der Klärung rechtlicher Fragestellung unterstützt werden.

Mitglieder des CCSR sind:

- Oliver Berndt, B & L Management Consulting GmbH
- Jürgen Biffar, DocuWare AG
- Thorsten Brand, Zöller & Partner GmbH
- Dr. Jens Bücking, Rechtsanwalt
- Stefan Groß, Peters, Schöneberger und Partner
- Wolfgang Heinrich, EASY SOFTWARE
- Carsten Heinmann, fme AG
- Peter Luzar, Consultec
- Gerhard Schmidt, Compario Media - Edition - Consult
- Peter Seiler, GID Global Information Distribution GmbH
- Dr. Dietmar Weiß, DWB Dr. Dietmar Weiß Beratung

- Contents of procedural documentation
- Management of retention periods
- Practical implementation of regulatory requirements

The CC "Taxation and Law" is the VOI-internal point of contact for all DMS-related legal issues. Its purpose is to transfer knowledge to members, improve the opinion-making process and create de facto standards. The involvement of supplier representatives, consultants, financial auditors and lawyers ensures an integrated approach.

Through publications, statements, conferences, road shows and individual answers to questions, the VOI-members and other interested parties will receive help with the clarification of legal questions.

Members of the CCSR are:

- Oliver Berndt, B & L Management Consulting GmbH
- Jürgen Biffar, DocuWare AG
- Thorsten Brand, Zöller & Partner GmbH
- Dr. Jens Bücking, lawyer
- Stefan Groß, Peters, Schöneberger und Partner
- Wolfgang Heinrich, EASY SOFTWARE
- Carsten Heinmann, fme AG
- Peter Luzar, Consultec
- Gerhard Schmidt, Compario Media - Edition - Consult
- Peter Seiler, GID Global Information Distribution GmbH
- Dr. Dietmar Weiß, DWB Dr. Dietmar Weiß Beratung

Sponsors

The VOI thanks the following companies who made this publication possible through their financial contribution:

DOCUWARE AG

Solutions for Integrated Document Management

DocuWare is a leading vendor of Enterprise Content Management software. Today DocuWare solutions are sold in more than 70 countries with a customer base of approx. 10,000 and more than 100,000 users.
Germering/Munich – Newburgh/NY – London – Paris – Barcelona – Campinas/Sao Paolo
www.docuware.com

EASY SOFTWARE AG

Having more than 10,500 customer installations, EASY SOFTWARE AG located in Mülheim an der Ruhr, Germany is a leading developer and provider of multi-platform solutions in the electronic archiving, document management and enterprise content management sectors.
www.easy.de