C/M/S/

Law.Tax

E-Archiving

TMT Sector Group

January 2010

We have become a knowledge society. Businesses' information and communications technology footprints grow daily, fuelled by the need to digitally store, access and communicate the ever growing volume of information and data they generate. As a result of this and the increase in online and cross-border transactions driven by technological development, the use of electronic documents and archiving systems is becoming more commonplace.

The legal framework relating to electronic archiving varies from jurisdiction to jurisdiction. This guide is intended to provide an overview of the law relating to electronic archiving across 17 European States, answering the most frequently asked questions for organisations operating in those countries.

For further information on the legal framework relating to electronic archiving, please contact any of the contributors to this guide or your usual contact at CMS.

Who we are

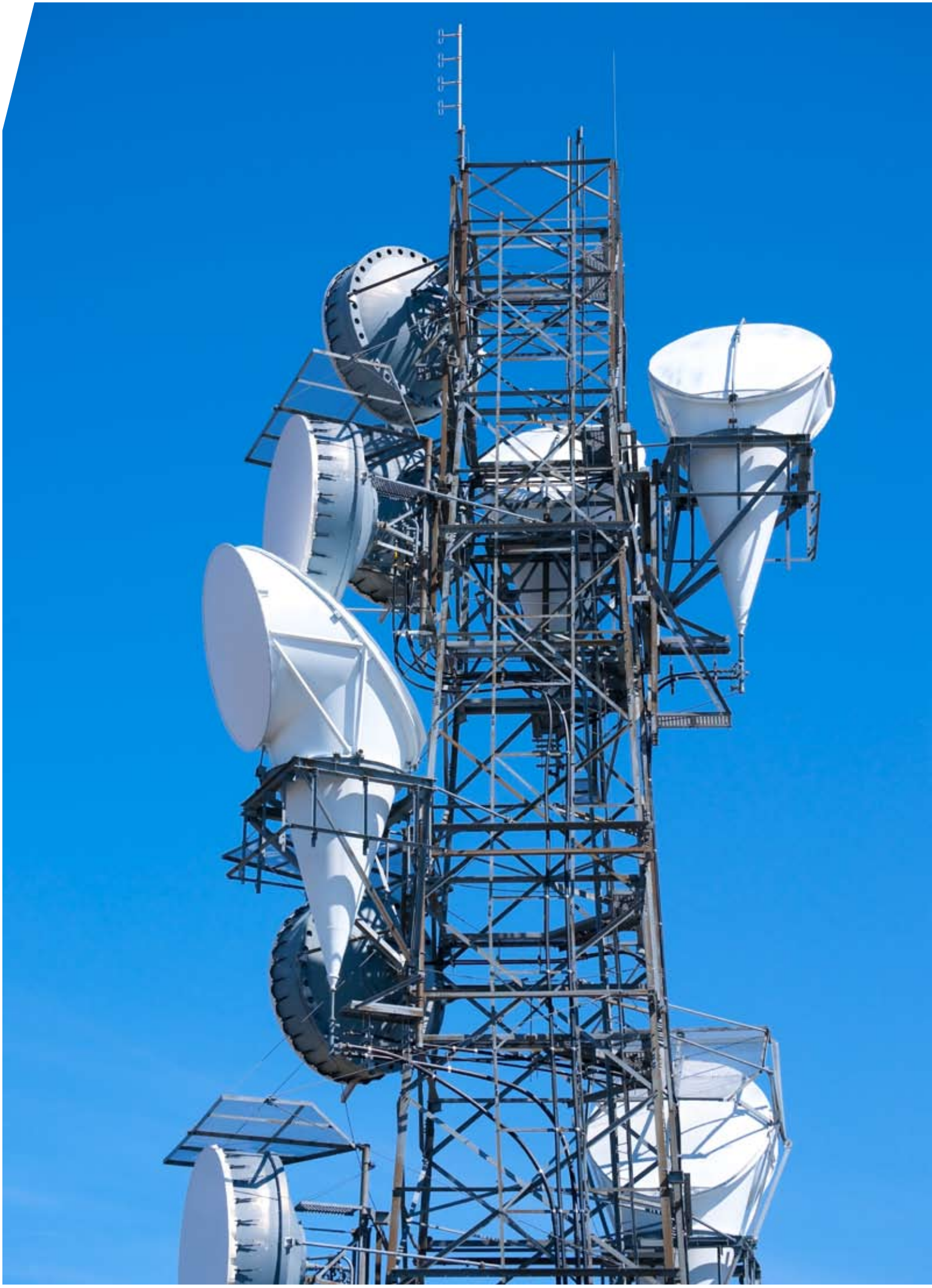
CMS aims to be recognised as the best European provider of legal and tax services that combines deep local expertise and the most extensive presence in Europe with cross-border consistency and coordination. CMS has a common culture and a shared heritage which make us distinctively European. CMS operates in 27 jurisdictions, with 53 offices in Western and Central Europe and beyond. CMS was established in 1999 and today comprises nine CMS firms, employing over 2,400 lawyers.

Our comprehensive understanding of our clients' businesses and markets allow us to consistently deliver sound, commercially relevant advice. We offer a wide range of expertise through 16 core Practice Area and Sector Groups both locally and across borders.

Data protection expertise

CMS advises on all aspects of data protection and security, confidentiality, privacy, human rights and freedom of information law. We are experts in the application of those laws across all industry sectors. We have extensive experience of advising public and private organisations on the use of data in their relationships with employees, customers, service providers, agents, regulators and the general public, including in connection with employee benefit arrangements, ICT infrastructures, contact centres, data warehousing arrangements, sales and claims operations and complaints processes and procedures.

We have a strong track record of working with customers and suppliers in relation to the provision of cross-border information and data management services to multinational organisations. Our international team advises in the collection, exploitation, protection, storage and disclosure of data, to assisting organisations to achieve their commercial and marketing objectives while remaining compliant under prevailing data protection rules in all the territories of operation.

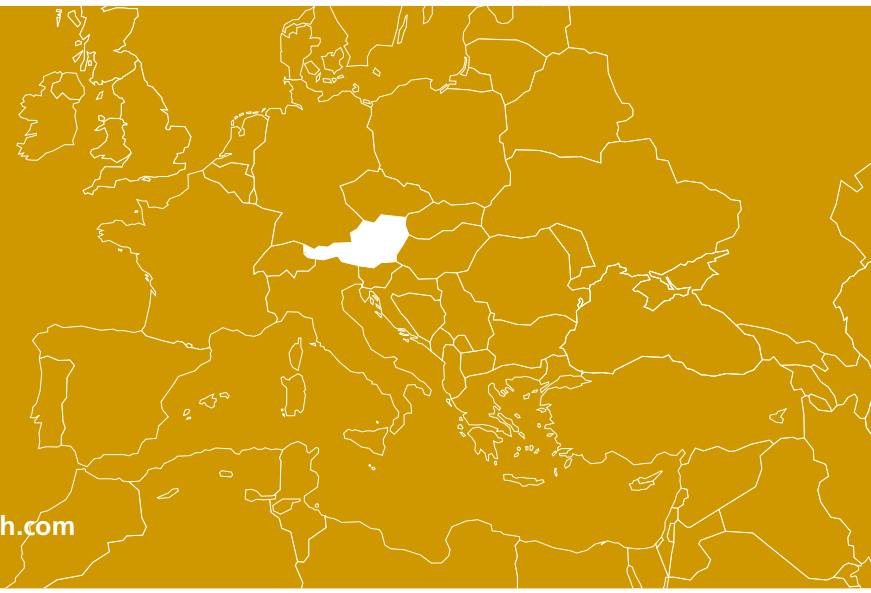


Contents

Austria	6
Belgium	11
Bulgaria	15
Croatia	20
France	25
Germany	30
Hungary	36
Italy	43
The Netherlands	51
Poland	55
Romania	60
Russia	66
Serbia	72
Slovakia	77
Spain	84
Ukraine	88
United Kingdom	91
List of Offices	96

Special thanks to Alex Le, Sarah Lloyd and Laura Hoyland for coordinating the production of this guide.

Austria



Johannes Juranek, johannes.juranek@cms-rrh.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving.

The legal framework regulating electronic archiving is set out in the following legislation:

Datenschutzgesetz (DSG)
Under the Austrian Data Protection Act (*Datenschutzgesetz* (DSG)) data protection is a constitutional right. The DSG only applies to personal data *(personenbezogene Daten)* which is interpreted widely and includes information relating to an individual's assets or creditworthiness. The subject of personal data may be a natural person, a legal entity, a partnership or other groups of people. The DSG applies to any use *(Verwendung)* of personal data, defined by law as

(i) data processing *(Verarbeitung)* and (ii) data transfer *(Übermittlung)*. Data processing *(Verarbeitung)* also includes data storage *(speichern, aufbewahren)*. Therefore, where the data being archived electronically is personal data, the requirements of the DSG must be satisfied.

In addition, certain laws (including certain labour laws) contain further regulations on data processing/storage. For example, provisions relating to the electronic storage of data may be found in the Austrian Telecommunication Act (TKG).

The EC Data Retention Directive 2006/24/EC
This Directive has not yet been implemented into Austrian law. Austria made a declaration postponing the application of Directive 2006/24/EC in respect of the retention of communications data relating to internet access, internet telephony and e-mail, for a period of 18 months from 15 September 2007. In addition, the requirement of Directive 2006/24/EC on the retention of communications data obtained from fixed and mobile telephony networks has not yet been implemented, despite the time limit for doing so having elapsed. The Austrian government has initiated a legislative procedure to amend the TKG, but concerns over data protection and human rights have delayed this amendment.

Accounting
The Austrian Commercial Act (*Unternehmergesetzbuch* (UGB)) provides that certain commercial documents (as specified in the UGB) may be archived electronically.

Tax
The Austrian Federal Tax Code (*Bundesabgabenordnung* (BAO)) contains a general provision permitting the electronic archiving of certain tax records.

Is there a legal definition of electronic archiving?

There is no strict definition of electronic archiving in Austrian law. The DSG definition of data processing *(Verarbeitung)* includes storing data *(speichern, aufbewahren)* and, therefore, electronic archiving. Consequently the data protection requirements of the DSG apply to electronic archiving. Data relating to individuals may be stored until the storage purpose is fulfilled (Section 6 Paragraph 1(5) DSG). Storing personal data without a specific purpose is considered illegal. The DSG does not specify a particular storage period for which personal data may be retained but states that such data should be destroyed "at the earliest possible" opportunity, subject to any legal requirement to retain this data.

In addition to the requirements of the DSG, certain tax and accounting laws also contain specific regulations on data storage, as set out below.

For accounting purposes, which records must be kept by corporations and for how long?

A corporation must keep its books, inventories, opening balances, annual accounts (including directors' report), group accounts (including the group directors' report), business letters received and copies of those sent and all accounting records (Article 212 Paragraph 1 UGB). For accounting purposes, the period for keeping these commercial records is generally seven years. If proceedings in connection with these commercial records are pending, the seven year period may be extended until the end of the proceedings. Parts of commercial records listed above may also be archived electronically (Article 190 UGB).

For tax purposes, which records must be kept by corporations and for how long?

A corporation must keep its books and records (Article 132 Paragraph 1 BAO). The term "books" includes all data necessary for the determination of taxable income by way of annual reports. The term "records" includes all other data defined by any other tax law provisions. In general, the commercial records to be kept for tax purposes are the same as those that must be kept for accounting purposes, i.e. company books, inventories, opening balances, annual accounts (including the directors' report), group accounts (including the group directors' report), business letters received and copies of those sent and all accounting records. These commercial records must be retained for a seven year period; however, if legal proceedings in connection with these commercial records are pending, the seven year period may be extended until the end of proceedings. Records may also be preserved through electronic archiving (Article 132 Paragraph 2 BAO).

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Any invoices and records referring to invoices must be kept for seven years from the date of issue or creation, as appropriate (Article 11 Paragraph 2 Austrian Act on Value Added Tax (*Umsatzsteuergesetz* – UStG)). Article 11 Paragraph 2 UStG also refers to Article 132 Paragraph 2 BAO which provides that these documents may be preserved through electronic archiving. In addition, Article 18 Paragraph 10 UStG provides for a 12 year storage period for all records for real estate properties. Directive 2001/115/EC has been implemented in Austrian law by an amendment to the UStG made on 31 December 2002.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Electronic copies of invoices and contracts have the same evidential value as paper documents.

Article 190 Paragraph 1 UGB and Article 131 Paragraph 3 BAO state that the electronic archiving of business letters (Article 190 Paragraph 1 UGB) and records (Article 131 Paragraph 3 BAO) is permitted. The terms "business letters" and "records" include invoices and contracts (*Torggler/Torggler* in Straube, Rechnungslegung, Section 189 HGB Rz 19; see also *Ritz*, Bundesabgabenordnung Section 132 Rz 5).

Electronic archiving is generally subject to the same requirements as non-electronic archiving of invoices and contracts. For both tax and accounting purposes, the law requires that documents can be reproduced that are identical in content to the original *(inhaltsgleich)*, that documents can be reproduced completely *(vollständig)* and in an ordered manner *(geordnet)* and, for accounting purposes, that documents can be reproduced as further originals *(urschriftsgetreu)* at anytime.

How long must documents be stored to cover the most important statutory limitation periods?

A corporation must keep its books, inventories, opening balances, annual accounts (including directors' report), group accounts (including the group directors' report), business letters received and copies of those sent and all accounting records (Article 212 Paragraph 1 UGB).
For accounting purposes, the period for keeping these

commercial records is generally seven years. If proceedings in connection with these commercial records are pending, the seven year period may be extended until the end of the proceedings. Parts of commercial records listed above may also be archived electronically (Article 190 UGB).

Any invoices and records referring to invoices must be kept for seven years from the date of issue or creation, as appropriate (Article 11 Paragraph 2 Austrian Act on Value Added Tax (*Umsatzsteuergesetz* – UStG)). Article 11 Paragraph 2 UStG also refers to Article 132 Paragraph 2 BAO which provides that these documents may be preserved through electronic archiving.

In addition, Article 18 Paragraph 10 UStG provides for a 12 year storage period for all records of real estate.

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

There are no specific regulations prohibiting the storage of electronic copies outside company premises (e.g. at a data centre). However, the storage of electronic copies abroad may be subject to certain limitations. In addition to any restrictions imposed for tax purposes, the DSG contains restrictions in connection with the transfer of personal data abroad. Article 12 Paragraph 1 of the DSG states that personal data may be freely transferred to a recipient located in an EU Member State. Article 13 DSG regulates the transfers of personal data abroad (as regards the requirement for the approval of the Austrian Data Protection Authority *(Datenschutzkommission)*. If personal data is being transferred to a non-EU Member State and the standard of data protection in that country is not comparable to the standard within EU Member States, permission is required.

For accounting purposes, Austrian law does not stipulate a specific location where electronic copies must be stored. The only stipulation is that electronic copies are readily available when required. Therefore, the place of electronic storage could be abroad (*Straube*, Rechnungslegung, Section 212 HGB, Rz 4).

For tax purposes, it is generally permissible to store all documents abroad, either on company premises or using a third party, provided that all such documents are readily available when required and storage of the documents within Austria is not required under other legislation (Article 131 Paragraph 1 BAO).

Austrian tax law requires all electronic copies to be available as and when required. Additionally, all "Basic Records" *(Grundaufzeichnungen)* on which the books and records are based must be transferred to Austria within a reasonable time of request and kept there from that time (Article 131 Paragraph 1 BAO). "Basic Records" are defined as records that form the basis for systematic recording of sales in the books (*Ellinger/Iro/Kramer/Sutter/Urtz* BAO Section 131 Anm.5). For electronic archiving, data collection protocols *(Datenerfassungsprotokolle)* and data transfer protocols *(Datenübernahmeprotokolle)* are defined as "Basic Records". However, these provisions might violate European law if EEA companies are obliged to keep their books in Austria (*Ritz*, BAO Section 131 Rz 3).

Directive 2001/115/EC has been implemented in Austria through the Second Amendment to the Austrian Tax Laws (2. *Abgabenänderungsgesetz*. 2002) and a Regulation of the Ministry of Finance (VO BGBl 2003/583).

Must special measures be taken to ensure data security?

Under the DSG, data protection is a constitutional right. Article 14 DSG sets out specific data security requirements. The DSG requires that, depending on the nature of the data being processed, all possible measures are taken to protect personal data from accidental or unlawful destruction or loss (taking into account the intended purpose of the processing, the cost of implementing such

measures and the state of technological development). In addition, the DSG requires that the processing of personal data must be lawful and that personal data must not be disclosed to unauthorised persons. Article 14 Paragraph 2 DSG sets out detailed provisions on the processing of personal data. Article 14 Paragraph 5 DSG prescribes a minimum three year storage period for protocol and documentation data.

The DSG only applies to personal data *(personenbezogene Daten)*. Personal data is interpreted widely and includes information on a data subject's assets and creditworthiness. The subject of personal data may be a natural person, a legal entity, a partnership or other groups of people.

The DSG makes a distinction between sensitive data *(sensible Daten)* and other personal data. Sensitive data is data that relates to a natural person's race and ethnic origin, political opinion, union membership, religion, health, sex and sexual orientation. The DSG provides that the confidentiality of sensitive data is extended beyond that of other data and sets out additional measures that should be taken to ensure the security of sensitive data.

Must special measures be taken to protect the data subjects' privacy?

Article 14 DSG sets out specific requirements that must be met to ensure the security of personal data held and protection of the subject's privacy. The DSG requires that, depending on the nature of the data being processed, all possible measures are taken to protect personal data from accidental or unlawful destruction or loss (taking into account the intended purpose of the processing, the cost of implementing such measures and the state of technological development).

Belgium

Tom Heremans, tom.heremans@cms-db.com
Lievin De Wulf, lievin.dewulf@cms-db.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

The legal framework regulating electronic archiving in Belgium can be summarised as follows:

The Belgian Data Protection Act of 8 December 1992 (Belgian Data Protection Act) The Belgian Data Protection Act applies to all forms of processing of personal data (data capable of identifying natural persons). As a general rule, personal data may only be processed under certain conditions, for example, with the consent of the data subject, in the framework of a contractual relationship, or if the processing is required to serve the legitimate interests of the data processor and does not affect the fundamental rights of the data subject (Article 5).

The processor of personal data must provide the data subject with the following information: the identity of the processor, the purpose(s) for which personal data is being processed and an explanation of the data subject's right to object to certain forms of data processing (Article 9).

The processor must also notify the Belgian Privacy Commission that it is processing personal data (Article 17). This notification can be carried out on-line via the Commission's website which is available at www.privacycommission.be.

EC Data Retention Directive The EC Data Retention Directive 2006/24/EC (Directive) has not yet been implemented into Belgian law. Belgium opted to postpone the application of Article 15(3) of the Directive for 36 months, concerning the retention of communications data relating to internet access, internet telephony and internet e-mail by communications providers. Despite this 36 month period elapsing on 15 March 2009, Belgium has yet to implement Article 15(3) of the Directive.

The Belgian Act on Electronic Communications (13 June 2005) The Act contains several provisions regarding the protection and retention of personal data in the telecoms industry. Telecoms operators may, for example, process subscriber or end-user traffic data but must delete those data as soon as they are no longer required for transmission services. Traffic data may also be used for marketing purposes provided the data subject consents and is given the opportunity to opt out of having their data processed for marketing purposes at the time a marketing communication is received. Traffic data must be deleted at the end of the marketing activity. Personal data required for invoicing purposes must also be deleted as soon as the term to collect the debt via legal proceedings has expired (Article 122).

Corporate Tax The Belgian Income Tax Code provides that all documents required to determine the taxable income of a Belgian taxpayer must be stored and made available to the tax authorities for seven years following the end of the taxable period. This also applies to all relevant files, software, management systems and the data within them.

VAT In principle, accounts, incoming and outgoing invoices and all other evidential documents must be stored in Belgium in their original format for seven years. For company accounts, this seven year period commences on 1 January of the year following the company's year end. In relation to invoices and other evidential documents, the seven year period commences on 1 January following the date of the invoices or other evidential documents. If the invoices or other documents relate to new buildings used in the taxpayer's business, these documents must be retained for a period of 15 years (Belgian VAT Code).

Electronic invoices may be stored in another EU Member State provided that full online access is available in Belgium and the relevant VAT authorities are notified beforehand.

In addition, the taxpayer must store all documentation relating to the electronic system and the software used to process the data for seven years starting from 1 January following the last year in which the system was used.

Is there a legal definition of electronic archiving?

There is no strict definition of electronic archiving established in Belgian law. However, the definition of personal data processing in the Belgian Data Protection Act is sufficiently broad to include the electronic archiving of personal data. Activities such as storing, saving, ordering or retrieving personal data are all acts of processing governed by the Belgian Data Protection Act.

For accounting purposes, which records must be kept by corporations and for how long?

Corporations must keep all commercial business records for a seven year period. Records must be dated and stored in an organised system (Article 6 of the Belgian Accounting Act of 17 July 1975).

For tax purposes, which records must be kept by corporations and for how long?

Corporate Tax All documents required for determining the taxable income of a Belgian taxpayer (i.e. books, documents and records as required for drawing up the accounts as well as all documents which have served for drawing up the accounts and other documents which are useful for determining the taxable income, e.g. tickets, inventory, meeting books, price offers, transportation documents, work sheets, order forms) must be stored for at least seven years following the end of the relevant taxable period, e.g. documents relating to the taxable period (accounting year) 2009 must be kept by the Belgian taxpayer until 31 December 2016.

The tax authorities may request to view all documents on which the taxpayer's taxable income is based. If the taxpayer fails to provide the requested documents within the requested time frame (normally one month, but in exceptional cases immediately), the tax authorities can apply an *"ex officio"* tax assessment *(imposition d'office/ aanslag van ambtswege)* meaning that they assess the amount of taxable income that they assume is received by the taxpayer based on information at their disposal.

VAT In principle, accounts, incoming and outgoing invoices and all other evidential documents must be stored in Belgium in their original format for seven years (15 where the invoices and other documents relate to new buildings used in the taxpayer's business) from 1 January of the year following the year in which the books are closed or the issue date, as appropriate (Belgian VAT Code).

The taxpayer must also store electronic system related documentation and software used to process the data for seven years from 1 January following the last year in which the system is used.

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Belgian VAT taxpayers are entitled to issue electronic invoices provided that those invoices are electronically signed or that a standard electronic data interchange code is used. Purchasers and suppliers must agree on the electronic invoicing method. No prior authorisation or notification to the tax authorities is required.

Such invoices must be created, communicated and stored in a format guaranteeing their authenticity. If security procedures are not sufficient to ensure the authenticity of the documents for at least seven years, a paper version of the invoice is required.

If the original invoices are on paper, the taxpayer must be able to demonstrate that the digitalized documents are a copy of the original invoices. In a circular letter of 13 May 2008 (Circ. AOIF 16/2008, E.T. 112.081), the tax authorities stipulated the conditions to be fulfilled in order to store incoming and outgoing invoices electronically. This list of conditions is fairly substantial and includes the following conditions: scanners must have a sufficiently high

image resolution, the scanned images should state the date and time of the scanning, the scanning software used must not allow the scanned images to be manipulated, the scanned images should be secured, the person carrying out the scanning must be identified, there must be a back-up policy and the originals must be kept at least one month following the scanning.

Given this substantial list of conditions, it should be verified whether a particular scanning procedure used is in line with the conditions set out in the circular letter. In addition, at any given time the taxpayer should be able to provide a detailed description of the software used and the procedures followed. This description should again comply with a minimum set of compulsory criteria. The circular letter specifies two types of scanning which comply with the conditions, i.e. scanning using an electronic signature and the scanning using a sealed algorithm.

The tax authorities may allow VAT payers to store their documents other than by hard copy at the taxpayer's official place of establishment if specific authorisation is obtained beforehand. Authorisation can only be obtained if storage of the documents at the official place of establishment leads to significant difficulties.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Electronic copies of agreements and invoices have the same evidential value as paper documents. The advantage of an original agreement or invoice, as regards the rules of evidence, is that the original document constitutes valid evidence, unless it can be established that the document has been falsified.

It is easier for a defendant to call into question the authenticity of an electronic document than an original document. If a defendant can establish reasonable doubt as to the electronic document's authenticity, the claimant will need to establish that the electronic document was created using a secure process and is thus a true copy of the original. In doing so, the claimant may put forward supporting evidence such as witness statements or confirmation that an agreement was executed as per the copy.

How long must documents be stored to cover the most important statutory limitation periods?

In principle, documents should be kept for seven years. This period starts on 1 January following the year in which the company books are closed or, in relation to invoices and all other non-book documents, the issue date. Invoices and other documents relating to new buildings that are used in the taxpayer's business should be kept for 15 years. Contractual documents should be stored until the end of the statutory limitation period of ten years (Article 2262bis of the Civil Code).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

All incoming and outgoing invoices which are stored electronically, must either be stored in Belgium or in another EU Member State provided that (i) full online access is available in Belgium and (ii) the competent VAT authorities are notified beforehand (Article 60, §3 of the Belgian VAT Code). Under Belgian VAT law, electronic invoices may not be stored outside the EU. The storage of invoices outside the EU is unlawful and may lead to administrative and criminal sanctions.

With respect to electronically stored incoming and outgoing invoices which are not located in Belgium, but which are, for instance, located in a foreign branch established in another EU Member State, there must be effective and full online access to these invoices at the place where the tax residency (i.e. *fiscal domicile*) of the taxpayer is established. The taxpayer must notify the VAT authorities in advance as to where these documents are stored. A copy of this letter will be sent by the VAT authorities to the tax receiver with respect to income taxes. Irrespective of where the documents are electronically

stored (at the tax residency of the taxpayer or in another establishment in Belgium or another EU Member State), the taxpayer must be able to show these documents at the tax residence of the taxpayer upon request.

If the taxpayer uses a data centre located in another EU Member State for storing the electronic incoming and outgoing invoices, the taxpayer must immediately inform the VAT inspector. Similarly, a copy of this letter will be sent by the VAT authorities to the tax receiver with respect to income taxes. In this case, the taxpayer must also be able to show these documents at the tax residence of the taxpayer upon request.

The Belgian Data Protection Act permits the transfer of personal data to a data centre in Belgium or within the EU, provided that an agreement is signed between the person responsible for the processing of this personal data (the taxpayer) and the processor (the data centre). The transfer of personal data outside the EU is only permitted if the recipient country offers the same level of protection for the data subject's personal data as EU Member States.

Where electronic invoices only contain information relating to companies and no personal data, the restrictions of the Belgian Data Protection Act will not apply.

Must special measures be taken to ensure data security?

With regard to non-personal information, both technical and contractual measures should be taken to secure non-personal information, such as concluding confidentiality agreements to prevent confidential information entering the public domain.

In relation to personal information, the Belgian Data Protection Act provides that the person responsible for processing personal data must adopt appropriate technical and organisational security measures to protect personal data against accidental or unauthorised destruction, accidental loss, alteration, access or any other unauthorised processing (Article 16 §4).

Where a data processor processes personal data on behalf of the personal data administrator, the personal data administrator must carefully select and supervise this data processor to ensure compliance with the personal data administrator's security requirements. In addition, the personal data administrator must enter into a written contract with the data processor (Article 16 §1).

Must special measures be taken to protect the data subjects' privacy?

In order to protect data subject privacy, the data controller should comply with the requirements of the Belgian Data Protection Act. This states that the processing of personal data must be legitimate (Article 5) and comply entirely with the following principles relating to data quality: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. Personal data must be relevant, not excessive, accurate, up to date, and kept no longer than necessary (Article 4 Belgian Data Protection Act).

The personal data administrator should not transfer personal data to countries outside the EEA that have not been officially recognised as providing an adequate level of protection (Article 21).

In addition, the data controller must respect the data subject's right to access, rectify, block and/or delete their personal data or object to their personal data being processed by the data controller (Articles 9 to 12 Belgian Data Protection Act).

Bulgaria

Zdravko Alexandrov, zdravko.alexandrov@cms-cmck.com
Boyana Bounkova, boyana.bounkova@cms-cmck.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving.

The legal framework governing electronic archiving in Bulgaria may be summarised as follows:

Personal Data Protection Act (PDPA) The PDPA sets out requirements relating to the processing (including storage) of personal data (information relating to individuals known as data subjects). The PDPA provides that personal data administrators should process and maintain such data according to the provisions of the PDPA after registering as personal data administrators with the Commission for Personal Data Protection (CPDP).

Electronic Communications Act (ECA) The ECA implements the provisions of the EC Data Retention Directive. The ECA entitles providers of public communication services and networks to collect and process user data, provided this data is related to the services being provided.

Providers of public communications services must retain certain data created or generated in the course of providing their services, for a 12 month period for the purpose of serious crime investigation. This includes data used for tracing and identifying the source, destination, date, time and duration of a communication as well as the type of communication and the user's communications terminal equipment (or what purports to be the user's communications terminal equipment) and the location label (cell ID).

Data relating to the contents of the communications may not be retained under the ECA. Furthermore, public communications services providers must destroy this data after 12 months. The data must be used in accordance with the terms and procedures established by the Special Intelligence Means Act and the Criminal Procedure Code.

Tax and Social Security Procedure Code (TSSPC) and Accountancy Act Companies are required to store certain accounting and commercial information relevant to the determination of their tax and social security liability. Such information may be stored either in hard copy or electronic form. In both cases, the information must be accessible for the revenue authorities in the event of an audit.

Value Added Tax Act (VAT Act) Invoices may be in paper or electronic form. It must be possible to guarantee the authenticity and integrity of both paper and electronic invoices, and they should remain legible. Invoices must be stored for five years following the expiry of the statutory limitation period for the relevant tax obligation.

Is there a legal definition of electronic archiving?

Bulgarian legislation does not provide a definition of the term 'electronic archiving'. However, the PDPA defines the storage of personal data as a type of personal data processing which may be carried out by automatic or manual means. Such personal data storage must be carried out in accordance with the requirements of the PDPA.

The PDPA defines personal data as any information relating to an individual who is identified or identifiable, directly or indirectly, by reference to an identification number or to one or more specific features.

For accounting purposes, which records must be kept by corporations and for how long?

Corporations must keep accounting information (in paper or electronic form) for the following periods:

— Payroll records: 50 years;

— Accounting and financial records: ten years;

— Documents for tax audits (including invoices and receipts for tax payments): five years after the expiry of the statutory limitation period for the relevant tax obligation. The statutory limitation period expires, as a rule, five years after the end of the relevant financial year;

— Documents for a financial audit: until the completion of the next financial audit; and

— All other (paper or electronic) documents: three years.

Accounting information on paper documents can be transferred into a technical (i.e. magnetic or optical) carrier. If such carrier allows the reliable reproduction of the information, the paper document can be destroyed (Article 42 of the Accounting Act).

For tax purposes, which records must be kept by corporations and for how long?

Accounting and commercial information, as well as any other information and documents relevant to taxation and mandatory social security contributions shall be kept by the company for the following periods:

— Payroll records: 50 years;

— Accounting and financial records: ten years;

— Documents for tax and social security audits (including invoices and other VAT documents): five years after the expiry of the statutory limitation period for the relevant tax or social security obligation. The statutory limitation period expires, as a rule, five years after the end of the relevant financial year;

— All other paper or electronic documents: five years.

(Article 38 of the TSSPC; Article 121 of the VAT Act)

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Invoices may be in paper or electronic form. The recipient of an electronic invoice must acknowledge receipt in order for the invoice to be admissible. It must be possible to guarantee the authenticity of the origin and the integrity of the contents of the electronic invoice. This can be achieved by using an advanced electronic signature under the EDESA. The authenticity and the integrity of the documents, as well as their readability must be guaranteed throughout the whole period of storage. Incoming and outgoing electronic invoices must be stored for the same period as paper invoices, i.e. five years after the expiry of the statutory limitation period for the relevant tax obligation. (Article 114, Item 6 and Article 121 of the VAT Act). The provisions of Directive 2001/115/EC have been implemented into Bulgarian law by the VAT Act.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

An electronic document signed with an electronic signature has the same evidential value as a paper document bearing a handwritten signature, unless the author or the addressee of the electronic document is a governmental or municipal authority. The electronic signature has the value of a handwritten signature with respect to all other third parties (Electronic Document and Electronic Signature Act (EDESA)).

For corporation tax purposes, an accounting expense is recognised for tax purposes when evidenced by a primary accounting document under the Accountancy Act (Article 10, Item 1 of the Corporate Income Tax Act). An accounting document, including a primary document, may be an electronic document complying with the requirements of the EDESA (Accountancy Act (Article 6, Item 2)).

For VAT purposes, the electronic invoice has the same value as a paper invoice if it complies with the requirements that receipt is acknowledged and the authenticity and integrity

of the document are guaranteed (Article 114, Item 6 of the VAT Act).

How long must documents be stored to cover the most important statutory limitation periods?

How long a document must be stored depends on the nature of the document. There are no specific provisions in the EDESA on how long documents and electronic communications should be stored. With regard to contractual documents, this would depend on the purpose and subject matter of the contract, its term and whether the parties intended to use it for evidential purposes.

There are more specific legal provisions with regard to documents relevant for determining the tax and social security liability of a company. The statutory limitation period for such liability normally expires five years after the end of the relevant financial year. Regardless of any possible tolling or renewal of the statutory limitation period, it will expire ten years after the end of the relevant financial year, unless the tax liability is deferred (Article 171 of the TSSPC). However, a company is required to store many documents that are relevant to its tax liability for periods beyond the expiry of the statutory limitation period (Article 38 of the TSSPC).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

There are no specific provisions stipulated in legislation with regard to the storage of non-personal information by companies.

With regard to personal information, the PDPA states that the personal data administrator may process personal data itself or it may assign the processing of personal data to a third party, which might also include storage of personal data. The transfer of personal data to a Member State of the EU or the EEA can be made with no restrictions. Transfer of personal data to a country outside the EEA is only permitted if the recipient provides an adequate level of protection for the personal data being transferred. The CPDP is authorised to decide whether the level of protection provided in the recipient third country is adequate.

There is no requirement that electronic documents must be stored in Bulgaria or within the EU for tax purposes. However, it must be possible to guarantee the authenticity of the origin and the integrity of the contents of the tax documents (including invoices), as well as their legibility during the whole period of storage (Article 121, Item 2 of the VAT Act).

All accounting and commercial information which the company is required to store for tax and social security purposes must be accessible for the revenue authorities in the event of a tax audit (Articles 38 and 39 of the TSSPC).

Must special measures be taken to ensure data security?

There are no general statutory provisions with regard special measures that must be taken to ensure the security of non-personal information. If non-personal information is classified as a trade secret or other confidential information, the security and non-disclosure of this information would be governed by contracts between the relevant parties or other regulations, depending whether they concern private companies or governmental institutions.

As regards personal information, under the PDPA, the personal data administrator must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorised access, alteration or dissemination, and against other unlawful forms of processing, which should comply with the latest technology and ensure a level of security corresponding to the risks involved in processing, and the nature of the data to be protected. The CPDP has adopted an Ordinance setting out the minimum level of technical and organisational measures that should be

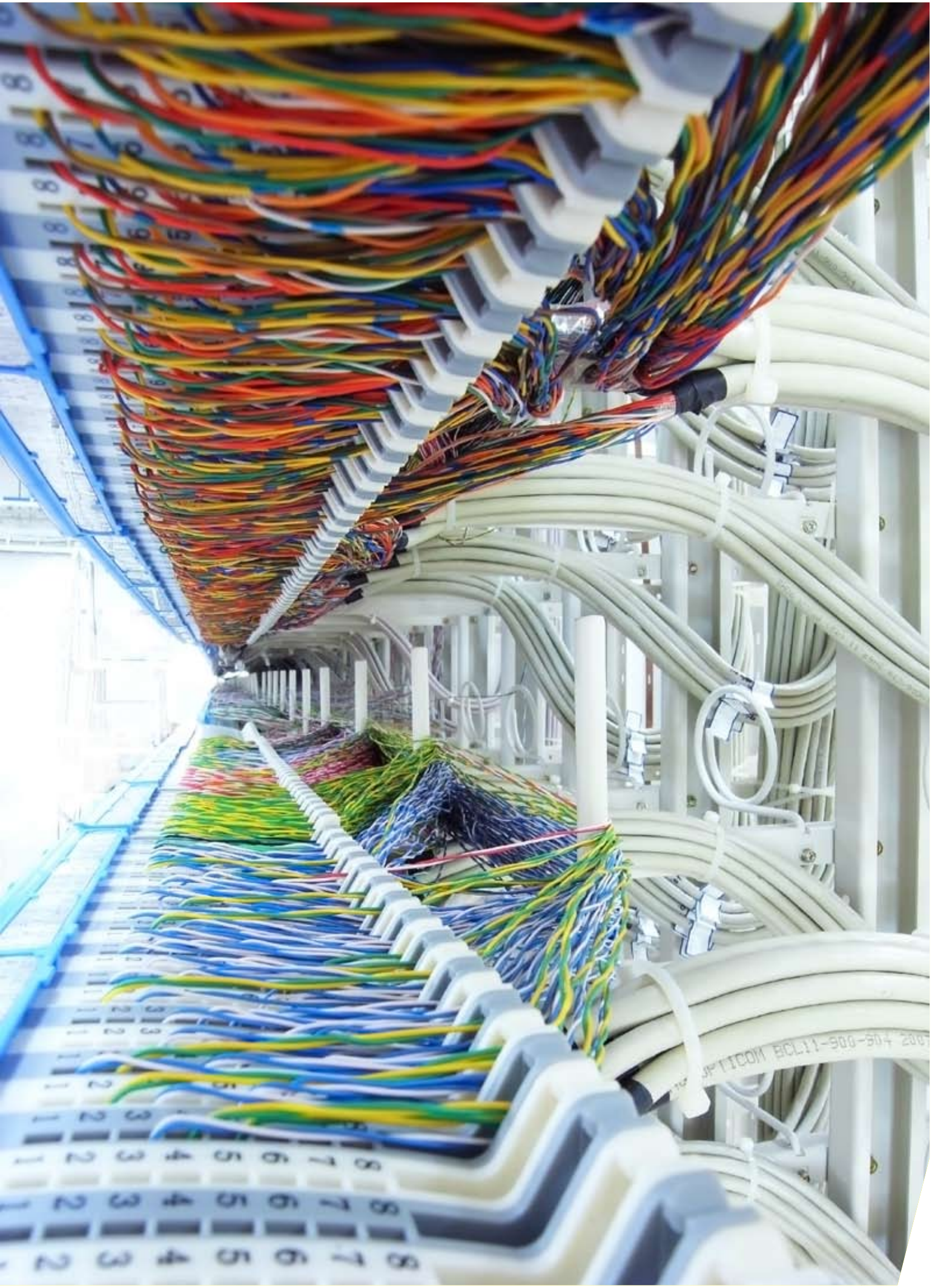
adopted by personal data administrators to ensure the security of personal data.

Must special measures be taken to protect the data subjects' privacy?

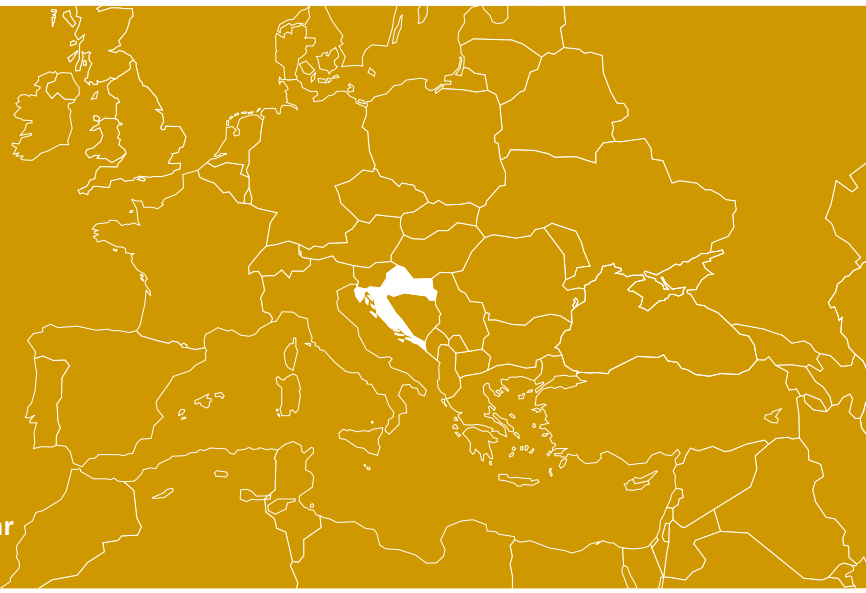
The PDPA states that the personal data administrator must only process and store personal data as long as it is necessary to achieve the purpose for data processing. Upon achievement of that purpose, the personal data administrator must either destroy the data, or transfer the data to another administrator after notifying the CPDP, provided that such transfer is provided for in statute and the purposes of processing are identical. In cases where, having achieved the purpose of personal data processing, the administrator wishes to store the personal data processed as anonymous data for historical, statistical or research purposes, it must inform the CPDP. The CPDP may prohibit such storage if the administrator has failed to provide sufficient protection for the anonymous storage of the data.

According to general principles of the PDPA, the data subject should provide consent before his/her personal data is processed. The data subject is entitled to access to his/her personal data and shall be entitled to request, at any time, that the personal data administrator removes, amends or blocks his or her personal data if the processing of this data does not comply with the provisions of the PDPA. The data subject is also entitled to object to the processing of his or her personal data if there are legitimate grounds for this objection. The data subject also has the right to object to the processing of his or her personal data for the purposes of direct marketing.

The PDPA provides for special and much stricter rules regarding the processing of "sensitive" personal data, i.e. data relating to an individual's racial or ethnic origin, political, religious or philosophical convictions, membership of political parties or organisations and associations having religious, philosophical, political or trade-union goals, health, sex life or human genome. "Sensitive" data may be processed only as long as the specific requirements of the PDPA are met.



Croatia



Marija Mušec, marija.musec@bmslegal.hr
Zrinka Vrtarić, zrinka.vrtaric@bmslegal.hr
Katarina Pavlek, katarina.pavlek@bmslegal.hr

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving.

The legal framework regulating electronic archiving is set out in the following legislation:

Croatian Personal Data Protection Act (PDPA) *(cro: Zakon o zaštiti osobnih podataka)* The aim of the PDPA is to protect the personal data of individuals. Individuals, companies, State and other bodies must comply with the provisions of the PDPA when processing individuals' personal data.

The PDPA definition of 'processing' personal data, which can be either manual or automatic, includes the archiving of personal data (cro: *spremanje*). Therefore, when personal data is archived electronically, the requirements of the PDPA must be met.

The Labour Act (cro: *Zakon o radu*) and The Insurance Act (cro: *Zakon o osiguranju*) contain further regulations on the archiving of personal data.

The Act on Electronic Communications (cro: *Zakon o elektroničkim komunikacijama*) The Republic of Croatia, whilst not yet a member of the EU, has incorporated the main provisions of the EC Data Retention Directive 2006/24/EC into the Act on Electronic Communications (cro: *Zakon o elektroničkim komunikacijama*).

The Croatian Accountancy Act (cro: *Zakon o računovodstvu*) provides that bookkeeping documents may be archived electronically.

The Croatian General Tax Act (cro: *Opći porezni zakon*) This Act sets out further provisions on the electronic archiving of data. Taxpayers who decide to keep their company books, registers and reports in electronic format are required to provide access to such electronically held information and ensure the proper storage, safekeeping and legibility of this information during the period prescribed in the Act.

Is there a legal definition of electronic archiving?

There is no legal definition of electronic archiving in Croatian law. However, the definition of personal data 'processing' in the PDPA includes the archiving of personal data (cro: *spremanje*). As such, the archiving of personal data must be carried out in accordance with the requirements of the PDPA.

For accounting purposes, which records must be kept by corporations and for how long?

Accounting documents:

— payroll and analytical records on salaries charged with compulsory contributions must be retained permanently;

— documents from which records have been taken into journal and ledger must be retained for a minimum of 11 years from the last day of the respective financial year;

— documents from which records have been taken into the sub-ledger must be kept for a minimum of seven years from the last day of the respective financial year.

(Article 7 of the Accountancy Act)

Business records:

— the journal and ledger must be kept for a minimum of 11 years from the last day of the respective financial year;

— the sub-ledger must be kept for a minimum of seven years from the last day of the respective financial year.

(Article 10 of the Accountancy Act)

For tax purposes, which records must be kept by corporations and for how long?

Incoming and outgoing invoices, documents relating to invoice corrections, evidence on export and import, documents relating to tax relief grants, tax assessments and all other documentation relevant for tax determination and payment must be kept for a minimum of five years from the expiration of the year to which the document refers. Documentation relating to real estate tax must be kept for a minimum of ten years from the end of the year to which the document refers (Article 24 of the VAT Act).

Records and documents on daily cash transactions, business records and accounting documents must be kept for ten years from the start of the statutory limitation period (Article 56 Paragraph 16 of the General Tax Act).

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

There are no special provisions in the VAT Act regulating electronic filing, but the electronic filing of business and other records and reports is permitted by the General Tax Act (Article 57 of the General Tax Act).

Incoming and outgoing invoices, whether stored electronically or on paper, must be kept for a minimum of five years from the end of the year to which they refer (Article 24 of the VAT Act).

Directive 2001/115/EC has not yet been implemented into Croatian law.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Croatian law regulating court and administrative proceedings does not stipulate that documents must be in paper form.

The use of electronic documents that are being submitted to different State bodies is governed by the Electronic Document Act. Electronic documents (either original or certified paper copies) that comply with all of the requirements of the Electronic Document Act may be used as evidence in proceedings before public bodies and arbitrations (Article 12 of the Electronic Document Act). Such electronic documents have the same legal validity as paper documents and may be equally used in all actions where the use of an original document or a certified copy is required. However, where a notarised copy of a paper document is required, an electronic document (its original or certified paper copy) cannot be used (Article 11 of the Electronic Document Act).

The use of an advanced electronic signature that records the time of a document's creation (a compulsory requirement for an electronic document being submitted to state bodies), is governed by the Electronic Signature Act. The electronic signature is considered legally valid, may be used in court proceedings and may not be contested solely on the basis that it is in electronic form (Article 6 of the Electronic Signature Act).

A contract may be concluded in electronic form (Article 293 of the Civil Code).

An accounting document may exist in electronic form. Such a document must contain either the name or other recognisable indicator of its authorised issuer or an electronic signature (Article 6 of the Accountancy Act).

How long must documents be stored to cover the most important statutory limitation periods?

The general limitation period for claims is five years (Article 225 of the Civil Code).

The limitation period for mutual claims arising from commercial contracts is three years (Article 228 of the Civil Code).

The limitation period for indemnification claims is three years, from the day the injured party becomes aware of the damage and the person who inflicted it. The right to claim indemnification is limited to five years from the day the damage occurred (Article 230 of the Civil Code).

In certain legal matters (e.g. as provided in the General Tax Act and Obligatory Social Contributions Act) there is a difference between the relative and the absolute limitation period. The relative limitation period is the resetting and restarting of the limitation period by any official action of the competent authority. The absolute limitation period refers to the ultimate period within which the competent authority must reach or enforce the final decision on the matter, regardless of the possible interruptions of the relative limitation period.

The relative (absolute) limitation period in tax matters is three (six) years, from expiry of the year in which the tax liability was incurred. The relative (absolute) limitation period for the tax authority to bring criminal proceedings is three (six) years, from the day the offence was committed (Articles 94 and 96 of the General Tax Act). The relative (absolute) limitation period for the calculation and charging of social insurance contributions, as well as for the initiation of criminal proceedings, is five (ten) years, from the day the limitation period first started (i.e. from the due days for calculation and payment of contributions, which are the same as the due days for the calculation and payment of salary).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Non-personal information There are no specific regulations prohibiting the storage of electronic copies outside company premises (e.g. at a data centre). Company books and other records, together with accompanying documentation, must be managed and stored so as to be accessible to the tax authorities, e.g.: (i) at the business premises, or (ii) with an authorised person, or (iii) with the taxpayer's accountant (Article 56 of the General Tax Act).

Where company books, records and reports are managed electronically and stored by a third party or abroad, taxpayers must make this information readily available to tax authorities, using either: (i) electronic media, (ii) modern telecommunication services, (iii) local (direct) connection or (iv) a long distance (indirect) connection with the taxpayer's system (Article 57 Paragraph 4 Point 5 of the General Tax Act).

Individuals' personal information Processing, including the storage of individuals' personal information, is governed by the PDPA. Personal data may only be transferred outside the Republic of Croatia if the recipient country or international organisation offers a satisfactory level of protection for personal data. If the standard of personal data protection in the recipient country or international organisation is uncertain, an opinion of the Croatian Data Protection Agency is required (Article 13 of the PDPA).

Directive 2001/115/EC has not yet been implemented into Croatian legislation. The present Croatian tax regulations do not contain any specific provisions on the storage of electronic invoices.

Must special measures be taken to ensure data security?

Non-personal information Where company books, records, reports and other data are managed electronically, a satisfactory level of protection, privacy and completeness must be ensured when providing access to these data by tax authorities (Article 57 Paragraph 3 of the General Tax Act).

Taxpayers must also, on request, provide tax authorities with documentation relating to the electronic system used for the electronic management of company books, records and reports. This documentation must include a description of the control system that prevents unauthorised additions, amendments to or deletions of electronically stored data (Article 57 Paragraph 6 of the General Tax Act).

With regard to an electronically maintained company ledger of the company, the Accountancy Act sets out the measures to be taken at the end of each financial year: exclusion of the possibility of any amendments to the ledger, possibility to print it on paper at any time with a valid electronic signature or printing the ledger on paper, binding in a manner which excludes the possibility of any amendments and having it signed by an authorised person (Article 10 of the Accountancy Act).

Individuals' personal information Personal data must be protected from accidental or intentional misuse, destruction, loss and unauthorised amendment or access.

Personal data must not be disclosed to unauthorised persons. Before personal data is transferred to third parties, the data subject must be informed and the following information must be detailed in writing: the purpose and legal grounds for the use of personal data and the type of requested personal data. The data controller must keep special records on personal data transferred to third parties, the third party (data processor) and the purpose of the data transfer.

Data that relates to a person's race and ethnic origin, political opinion, union membership, religion, health, sex or commission of an offence (including proceedings) may only be processed with the data subject's consent for the specific purpose for which such consent has been obtained (PDPA).

Must special measures be taken to protect the data subjects' privacy?

Individuals, companies, State and other bodies must satisfy the requirements of the PDPA when processing the personal data of individuals.

Personal data must not be retained for longer than is necessary to fulfil the purpose for which the data is being processed. Once this purpose has been fulfilled, such data must be deleted. Where personal data is stored for a longer period of time for historical, statistical or scientific purposes, special protection measures must be taken (PDPA) to secure the data held.

The data controller must provide the data subject with the following information: the data controller's identity, the purpose for which personal data is being processed, details of any third parties to whom personal data may be transferred, the nature (i.e. whether voluntary or compulsory) of the data processing and the data controller's legal grounds for processing the personal data.

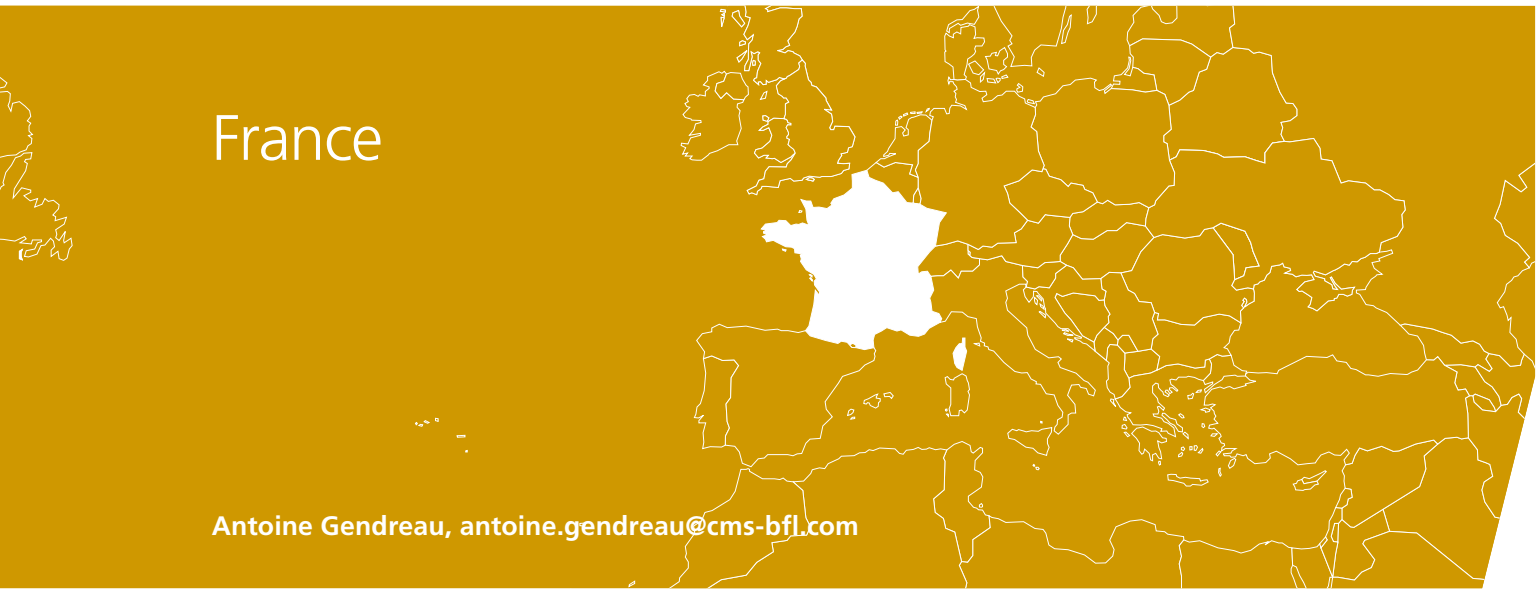
Where data processing is carried out on a voluntary basis, the data subject has the right at any time to withdraw his consent to his personal data being processed and to request that his personal data is no longer processed, except when his personal data is being processed for statistical purposes and the data subject cannot be identified from such data.

The data controller must complete, amend or delete all incomplete, inaccurate or obsolete personal data both as a matter of course and at the data subject's request.

Personal data must not be disclosed to unauthorised persons. Before personal data is transferred to third parties, the data subject must be informed and the following information must be detailed in writing: the purpose and legal grounds for the use of personal data and the type of requested personal data. The data controller must keep special records on personal data transferred to third parties, the third party (data processor) and the purpose of the data transfer.

Personal data may only be transferred outside the Republic of Croatia if the recipient country or international organisation offers a satisfactory level of protection for the personal data being transferred. Where the standard of personal data protection in the recipient country or international organisation is uncertain, an opinion from the Croatian Data Protection Agency is required.

France



Antoine Gendreau, antoine.gendreau@cms-bfl.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

The legal framework regulating electronic archiving can be summarised as follows:

Act n° 2000-230 of March 13, 2000 This sets out requirements relating to the adaptation of evidence rules for information technologies, in particular with regard to electronic documents and electronic signatures, leading to Article 1316-1 of the Civil Code. This provides that a document in electronic form is admissible as evidence in the same manner as a paper document, provided that the addressor can be duly identified and the electronic document can be formatted and stored so as to ensure its integrity. However, the Act does not provide clarification as to the form or means of electronic archiving.

Norm NF 42-013 (a non-legally binding provision published by the French Association of Normalisation (AFNOR)) provides electronic archiving guidance, including a technical specification. This includes Norm NF 42-013 which recommends the use of a WORM ("write once read many") support system for electronic archiving to ensure that recorded data cannot be modified.

EC Data Retention Directive (2006/24/EC) National measures implementing the EC Data Retention Directive (2006/24/EC) were notified in September 2007 and early 2008. However, these measures have not yet been adopted and therefore the Directive has yet to be implemented into French law.

The French Data Protection Act The French Data Protection Act defines the 'storage' of personal data as a type of personal data 'processing'. Such personal data storage must be carried out in accordance with the requirements of the Act.

Is there a legal definition of electronic archiving?

There is no strict definition of electronic archiving in French law. However, the French Data Protection Act defines the 'storage' of personal data as a type of 'processing' (any operation or set of operations in relation to personal data, which includes the obtaining, recording, use and storage of such data) (Article 2, French Data Protection Act).

Where personal data (information relating to an individual who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him) is being archived, such archiving must be in accordance with the requirements of the Act.

For accounting purposes, which records must be kept by corporations and for how long?

Companies must keep all accounts documents to which the authorities may access, such as account books and registers, for a six year period from the latest transaction stated in the accounts book or from the date on which the document was set up (Article L. 102 B, I- Paragraph 1 of Tax Procedure Code within the meaning of *"Livre de Procédure Fiscale"*).

There is a specific requirement with regard to documents set up or received electronically. Such documents must be stored in their original electronic format for three years and for a following three-year period in any format.

For tax purposes, which records must be kept by corporations and for how long?

Outgoing electronic invoices must be stored in their original format in a suitable system for three years (a tax audit may be carried out within three years of the date of sending)

and for the following three years they may be stored in any format.

Incoming invoices (companies which use the invoices for justifying the right to deduct VAT) must be kept in their original format for six years (for VAT purposes).

For VAT purposes, balance ledgers (receipts and expenses) must be kept for three years plus the outstanding year. Contracts, vouchers, credit notes and receipts must also be kept for the same period.

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Companies that issue or receive dematerialised invoices must keep them in any format for six years. This period runs from the date stated on the invoice that corresponds to the date of issue of the invoice.

A sequential list of such invoices must be kept summarising the following information:

— reference number and date of invoice;

— date and time of message (the details set out in the dematerialised invoice);

— net amount, total tax and currency code when the invoice is not in Euros;

— information identifying the issuer and recipient of the invoice as provided by the tele-transmission service (code, name, SIRET number, address, capacity of supplier and client);

— details of the software version used for the dematerialisation of the invoices.

This list of information, provided by the electronic system, must specify any errors occurring during transmission.

Where the function is outsourced, the service provider responsible for invoicing on behalf of the company must maintain such a list for the company.

Companies must keep and update a list of companies with which they exchange invoices. This list can be maintained electronically or manually. If kept electronically, the company must ensure that data in this list cannot be altered and must update the list each time any invoices are issued. If held manually, the list must be printed out sequentially at least once daily, according to the date of receipt or issue of the invoices.

On request, companies must be able to provide invoices to the French tax authorities without delay.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Contracts created in electronic format, (as opposed to electronically archived hard copy contracts) have the same evidential value as hard copy documents provided the issuer can be identified and the documents are created and stored in a manner that ensures the integrity of the documents are maintained (Article 1316-1 of the French Civil Code).

As there are no legal provisions regulating electronic copies of contracts originally entered into in hard copy, the Civil Code's general provisions on the admission of copies in place of original documents apply. Copies, when the original document still exists, only have evidential value insofar as they evidence the contents of the original, the production of which can still be requested (Article 1334 Civil Code).

A copy can be put forward instead of the original if the latter has been lost following an act of God or the original has not been archived and a copy is provided that not only corresponds faithfully to the original but is sustainable, on the basis that it is an indelible copy of the original (Article 1348 Civil Code). The judge has a discretionary power to decide whether a copy complies with these criteria. As the

burden of proof relating to the criteria of "faithfulness" and "sustainability" is so high, an expert is often appointed by the judge to evaluate the "faithfulness" and "sustainability" of the copy document.

How long must documents be stored to cover the most important statutory limitation periods?

The period of time for which documents must be stored depends on the nature of the particular document.

In civil matters, the statutory limitation period is five years for in *personam* actions (Article 2224 of the Civil Code) and 30 years for *in rem* actions (Article 2227). For commercial matters, the statutory limitation period is five years (Article L. 110-4 of the Commercial Code). For revenue matters, it is six years (Article L. 102B of the Tax Procedures Code).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Electronic copies and electronic invoices may be stored at the premises of the company or by a third party located in another country. The country of storage need not be located within the EEA provided that adequate levels of protection are ensured for such data, in compliance with European Commission standards. The French Data Protection Agency (*Commission Nationale de l'Informatique et des Libertés* – CNIL) website provides information on compliance with the level of personal data protection by country.

Electronic invoices must be stored in France, in another EU Member State or in a country bound by a mutual administrative assistance treaty with France.

Individuals' personal information must be stored in a country that provides adequate levels of protection for that data in accordance with European Commission standards. The decision of the French Data Protection Agency (*Commission Nationale de l'Informatique et des Libertés* – CNIL) of 11 October 2005 sets out further information on data protection standards.

Must special measures be taken to ensure data security?

Non-personal information is generally protected by a confidentiality obligation that is enforced by the company where archives are kept at the premises of the company or, if archiving is carried out externally by a third party, such a confidentiality obligation will be contained in the contract entered into between the company and the archiving third party.

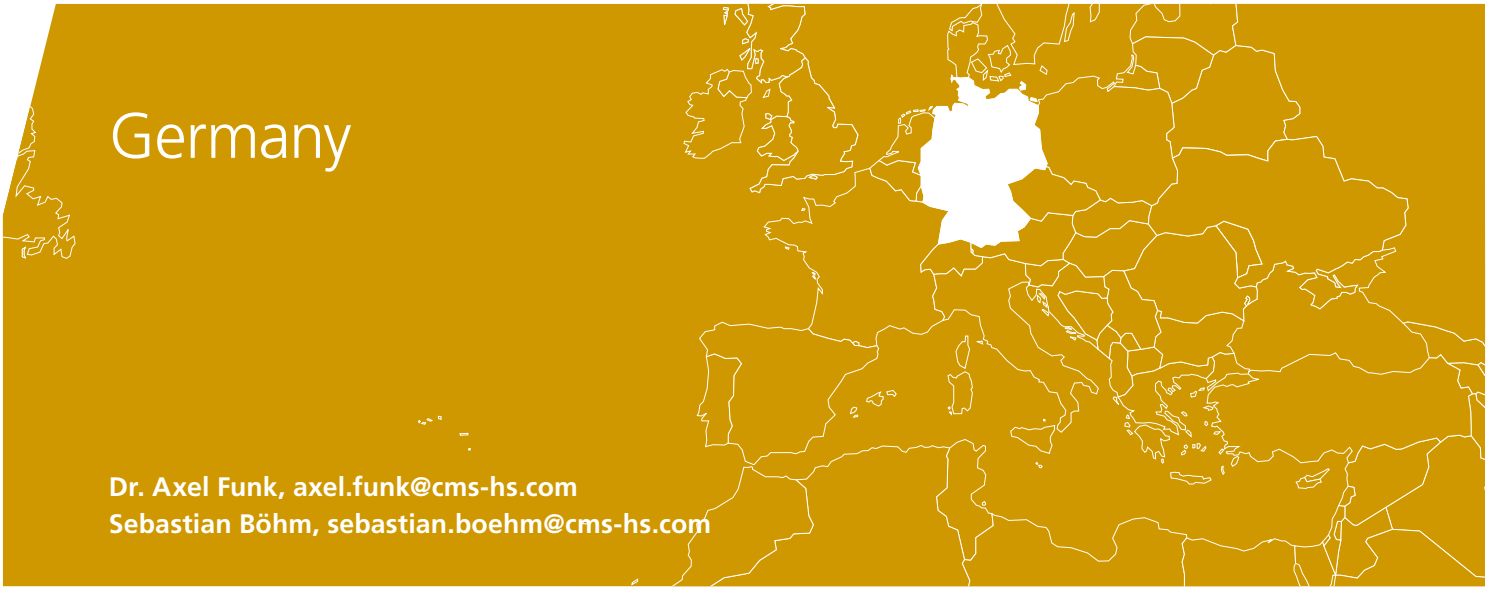
With regard to personal data, Act No 78–17 provides that the data controller must implement appropriate measures to ensure the security of such data. The data controller must take precautions, taking into account the nature of the data and the risks associated with the processing of the data, to secure and protect the data from alteration and damage, or access by non-authorised third parties (Article 34 of Act No 78–17). However, the Data Protection Act does not specify the measures that must be taken. The CNIL recommends that personal data relating to an individual's health should be stored using a coding system in order to keep such data confidential.

Must special measures be taken to protect the data subjects' privacy?

The CNIL recommendation of 11 October 2005 (n°2005–213) concerning individuals' personal information, recommends that all third party archiving service providers should adopt appropriate technical measures to ensure that the personal data contained in archived documents is only accessible by authorised persons and is protected against modification or destruction. Access to personal data should be restricted, taking into account the sensitivity of the data and the risks associated with processing such data.

The CNIL recommends that personal data is only stored for the period of time necessary to fulfil the specific purpose for which it has been retained. It also recommends additional measures are taken in relation to the archiving of sensitive personal data, (i.e. data relating to a person's health or religious beliefs). One such measure recommended by CNIL is the anonymisation of such sensitive personal data.

Germany



Dr. Axel Funk, axel.funk@cms-hs.com
Sebastian Böhm, sebastian.boehm@cms-hs.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

Listed below are some key legal provisions for electronic archiving.

The Federal Data Protection Act *(Bundesdatenschutzgesetz)* This regulates the automated processing (including collecting and storing) of personal data (any information concerning the personal or material circumstances of an identified or identifiable natural person) by public and private bodies. Storage of personal data is only permitted if it is justified by law or with the consent of the data subject. According to the attachment to Section 9 of the Federal Data Protection Act, certain measures must be taken to ensure data protection and data security.

Tax For tax purposes, there is no comprehensive statutory framework regulating electronic archiving. The more specific provisions are included in the rules of orderly bookkeeping (*Grundsätze ordnungsmäßiger Buchführung* – GoB and *Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme* – GoBS) and the principles of data access and auditing of digital documents (*Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen* – GDPdU). It is essential to ensure that documents archived electronically cannot be altered and may be accessed at any time.

Telecommunications Act (*Telekommunikationsgesetz*) The EC Data Retention Directive (2006/24/EC) has been implemented into German law by Sections 113a and 113b of the Telecommunications Act *(Telekommunikationsgesetz)*.

Providers of public telecommunication services are obliged to store certain data where this is generated or processed by the provider. Where the provider does not generate or process such data, it must ensure that this data is retained and must disclose the location of where this data is retained, upon request (Section 113a of the Telecommunications Act).

The data that must be stored under Sections 113a and 113b of the Telecommunications Act includes information gathered from fixed or mobile telephone networks, the internet, e-mail and SMS. This includes information relating to a call or internet use, such as the time of the call or use, its source number or IP address, the destination phone number, e-mail addresses, the geographical location of mobile phones in a call and the duration of such communications. All data stored according to the EC Data Retention Directive must be retained and made available for six months.

An appeal to the Constitutional Court regarding the question of whether Sections 113a and 113b of the Telecommunications Act are constitutional has been filed by over 34,000 people and is yet undecided.

Is there a legal definition of electronic archiving?

There is no strict legal definition of electronic archiving in German law. The Federal Data Protection Act applies to the "automated processing" (the collection, processing or use of personal data by means of data processing systems) of "personal data" (information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)). The processing of personal data includes the "storage" (the entry, recording or preservation of personal data in a storage system for future processing or use) of personal data (Section 3 of the Federal Data Protection Act).

For accounting purposes, which records must be kept by corporations and for how long?

Section 257 of the Commercial Code *(Handelsgesetzbuch)* requires corporations to keep the following documents:

— commercial business records, inventories, opening balance sheets, annual financial statements, management reports, consolidated statements of affairs as well as procedural instructions and other organisational documents necessary for interpreting such documents and accounting records for ten years from the end of the calendar year in which the records were created;

— incoming business correspondence and copies of mailed business correspondence for six years from the end of the calendar year in which the correspondence was received or mailed.

With the exception of opening balance sheets and financial statements, all of the above documents may be archived digitally.

For tax purposes, which records must be kept by corporations and for how long?

Section 147 of the Fiscal Code *(Abgabenordnung)* requires corporations to keep the following documents:

— commercial business records, inventories, annual financial statements, management reports, opening balance sheets and other organisational documents necessary for interpreting such documents, accounting records and certain customs documents for ten years from the end of the calendar year in which the records were created;

— incoming business correspondence, copies of mailed business correspondence and other documents material for taxation purposes for six years from the end of the calendar year in which the records were created respectively in which the correspondence was received or mailed.

With the exception of financial statements, opening balance sheets and customs documents, all of the above documents may be archived digitally.

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Section 14b of the Value Added Tax Code *(Umsatzsteuergesetz)* requires corporations to keep incoming invoices and copies of outgoing invoices for ten years from the end of the calendar year in which the invoice was issued. There are no specific VAT rules for the electronic storage of invoices; the general rules of Section 147 of the Fiscal Code apply.

Electronic storage must conform with the rules of orderly bookkeeping (*Grundsätze ordnungsmäßiger Buchführung* – GoB and *Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme* – GoBS) and the principles of data access and auditing of digital documents (*Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen* – GDPdU), meaning that copies must be readily accessible and exact copies of incoming invoices and reproductions of outgoing invoices must be maintained.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Electronic copies of contracts do not have the same evidential value as paper documents. Whilst signed original hard copy documents are deemed authentic under Section 416 of the Code of Civil Procedure *(Zivilprozessordnung),* the authenticity of electronic copies of contracts is determined at the court's discretion.

Digital contracts that have been entered into using advanced digital signatures are deemed authentic unless proven otherwise (Section 371a of the Code of Civil Procedure *(Zivilprozessordnung)*).

For certain declarations, such as notice of termination of a work contract, a hard copy document is mandatory as a digital copy has no evidential value in such cases.

Where electronic storage of documents conforms to the rules of orderly bookkeeping (*Grundsätze ordnungsmäßiger Buchführung* – GoB and *Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme* – GoBS) and to the principles of data access and auditing of digital documents (*Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen* – GDPdU), electronic copies of invoices have the same evidential value as paper documents in conflicts with the fiscal authorities.

How long must documents be stored to cover the most important statutory limitation periods?

The period of time for which a document must be retained varies, depending on the nature of the document. Most statutory limitation periods in Germany are two years (e.g. the standard warranty period for sales contracts) or three years (the standard statutory limitation applicable for most claims), some limitation periods are five years (e.g. the standard warranty period for the purchase of real estate). The longest statutory limitation periods in Germany are 30 years (e.g. for claims which have been validated by a court decision).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Section 146 of the Fiscal Code *(Abgabenordnung)* requires that all documents kept for tax purposes must be stored in Germany. However, there is no obligation to store the document on company premises, meaning that such documents may be stored by third parties.

Individuals' personal information may be transferred to and stored in any EU country. Transferring personal information to countries outside the EEA is only permitted if the respective country or the recipient maintains an adequate level of data protection (e.g. the safe harbour programme for recipients located in the USA).

Personal data may be stored by third party agents provided that this is recorded in writing, specifying amongst other things, the purpose and duration of the arrangement with the agent, the scope of the processing and intended use of the data, the technical and organisational measures to be taken to secure the data and the principal's right to supervise and instruct the agent and any subcontractors (Section 11 of the Federal Data Protection Act). The responsibility for compliance with the Federal Data Protection Act rests with the principal.

For tax purposes, electronic copies of invoices must be stored in Germany unless they can be accessed remotely, in which case they may be stored in any EU country. However, there is no obligation to store the documents on company premises, meaning that such documents may be stored by third parties.

Must special measures be taken to ensure data security?

For accounting and tax purposes, the rules of orderly bookkeeping (*Grundsätze ordnungsmäßiger Buchführung* – GoB and *Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme* – GoBS) and the principles of data access and auditing of digital documents (*Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen* – GDPdU) apply, requiring that extensive precautionary measures are taken to prevent the loss or modification of data.

Where personal data is processed by automatic means, appropriate measures should be taken, depending on the type of personal data to be protected, for:

— preventing access by unauthorised persons to data processing systems in which personal data are processed (access control);

— ensuring that those authorised to use a data processing system can only access personal data as permitted by their level of authorisation and that personal data cannot be viewed, copied, amended or removed without authorisation either during processing or after saving (user access control);

— ensuring that personal data cannot be viewed, copied, amended or removed without authorisation during electronic transmission or transit or whilst personal data is saved on data carriers, and that the offices from which personal data may be transmitted using data transmission facilities can be monitored (transmission control);

— ensuring there is a system in place for ascertaining whether personal data has been accessed, amended or removed from data processing systems and by whom (input control);

— ensuring that personal data being processed on behalf of other parties is processed only in line with client instructions (order control);

— ensuring that personal data is protected against accidental destruction or loss (availability control);

— ensuring that data is only processed for the purpose for which it was captured.

Must special measures be taken to protect the data subjects' privacy?

When collecting personal data, the data controller must define the purpose of the data collection. Use of any personal data collected is in general limited to the purpose for which it has been collected and processing for any other purpose is prohibited. The Federal Data Protection Act provides that personal data must be deleted if the purpose for which it was collected has been fulfilled.

The collection and processing of personal data is only permitted if it is justified by law or the consent of the data subject has been obtained. According to Section 4a of the Federal Data Protection Act, the data subject's consent must be given in writing unless special circumstances warrant the giving of consent in another form. If the consent is to be given together with other written declarations, e.g. the consent is contained in a contract provided by the data controller, the consent must be clearly distinguishable. Failure to comply with this written form requirement will invalidate the consent. The data controller must provide the following information in advance: (1) the identity of the data controller, (2) the purpose of collection, processing or use and (3) the categories of recipients to whom the data may be transferred, if in the circumstances, there are no grounds for the data subject to assume that data will be transferred to such recipients.

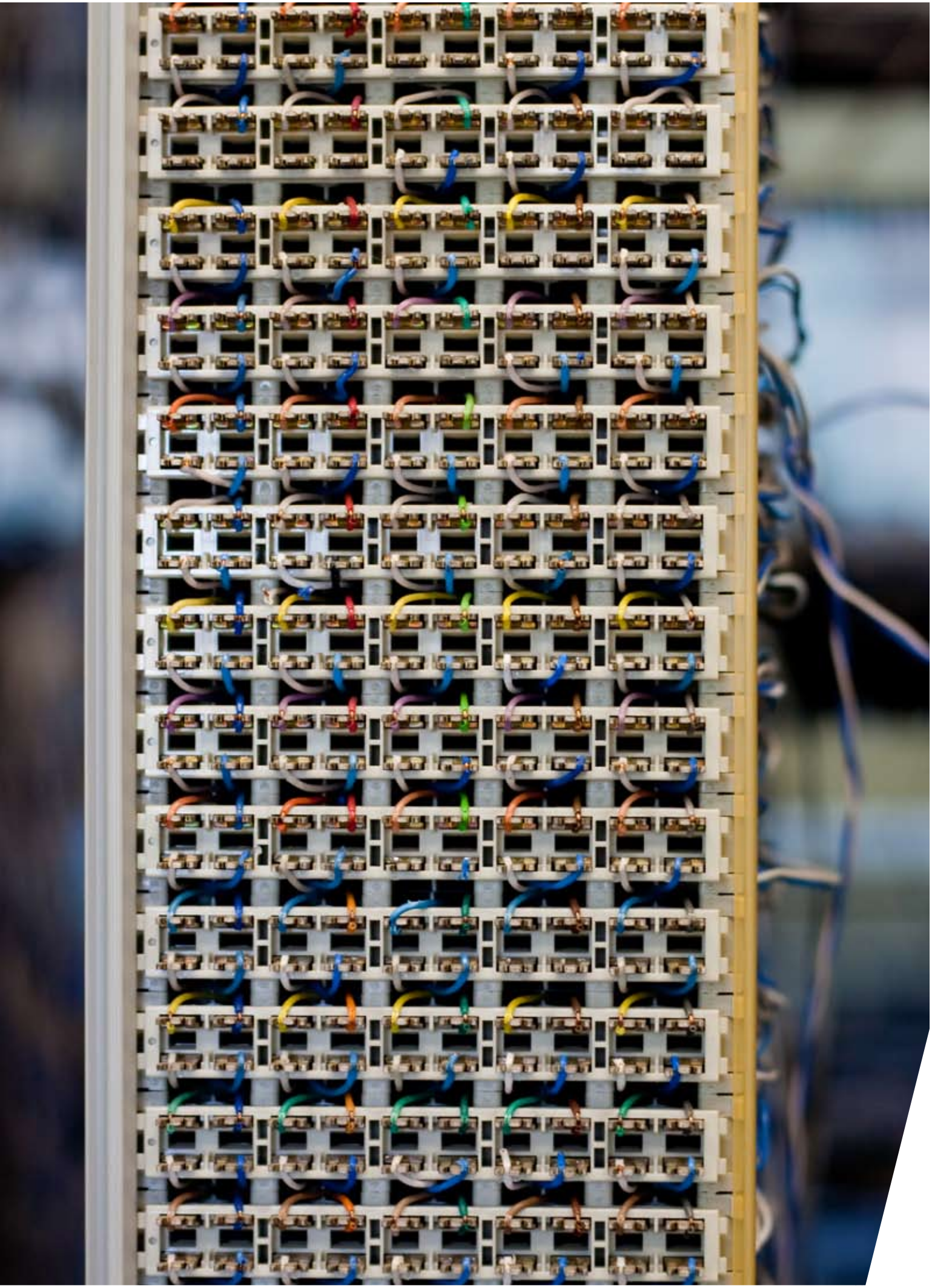
The most important provision permitting data collection by private bodies under the Federal Data Protection Act without the data subject's explicit consent is Section 28, permitting the collection of personal data for the purpose of entering into and performing a contract with the data subject. Furthermore, Section 3a of the Federal Data Protection Act sets out the general principles of data reduction and data economy, namely that the collection and retention of personal data must be limited to the data that it is necessary to retain for a specific purpose.

Where personal data is stored for the first time without the knowledge of the data subject, the data subject must be notified of such storage, the type of data being stored, the purpose for its collection, processing or use and the identity of the data controller. The data controller must correct the personal data it holds if notified by the data subject that it is incorrect. In the event that the data subject disputes the correctness of personal data stored, such data must be blocked if it is not possible to ascertain whether the data is correct or incorrect.

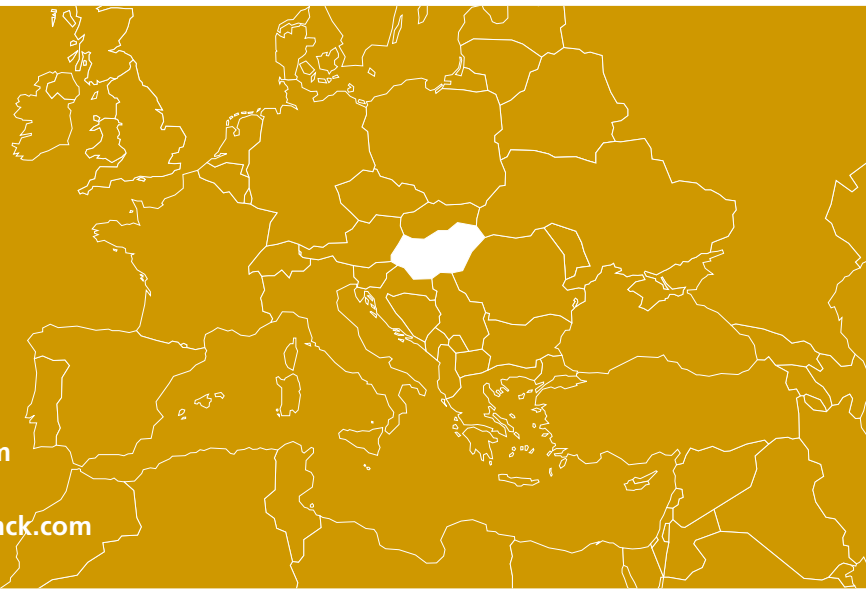
As the transfer of personal data to third parties is classed as data processing under the Federal Data Protection Act, such a transfer is only permitted if justified by law or the consent of the data subject has been obtained. The transfer of personal data to third parties is only justified by law in a limited number of cases. The data controller seeking to transfer personal data must establish that the transfer is either for the purpose of fulfilling obligations arising under

a contract with the data subject; or is necessary to safeguard the justified interests of the data controller or a third party and there is no reason to assume that the data subject has an overriding legitimate interest in its data being excluded from transfer; or that the transfer is necessary for certain scientific research.

German data protection law does not provide for an inter-company group privilege. The transfer from one legal entity to another legal entity within the same group is subject to either justification by law or prior consent of the data subject.



Hungary



Dóra Petrányi, dora.petranyi@cms-cmck.com
Balázs Kökény, balazs.kokeny@cms-cmck.com
Tamás Fehér, tamas.feher@cms-cmck.com
Márton Domokos, marton.domokos@cms-cmck.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

The legal framework regulating electronic archiving can be summarised as follows:

E-Archiving Decree Decree No.114/2007 (XII.29.) GKM (Ministry of Economy and Transport) on Electronic Archiving (E-Archiving Decree) states that documents may be archived electronically, provided:

— the documents cannot be modified;

— the documents remain legible;

— the documents are protected against unauthorised access, modification, deletion or destruction; and

— the documents are signed using an advanced electronic signature *(fokozott biztonságú elektronikus aláírás)* or stored in a "closed storage system" *(zárt megőrzési rendszer)* and this system is approved by an accredited certifying institution.

If a document is signed using an advanced electronic signature *(fokozott biztonságú elektronikus aláírás)*, an archiving service provider may be used for document retention. If the document does not contain an advanced electronic signature, it can only be stored in a system that is certificated for this purpose by an authorised institution, attesting that the system meets all safety standards required for the retention of electronic documents. Where the duration of the required retention period exceeds 11 years, the E-Archiving Decree sets out further requirements for the archiving process.

E-Signature Act Detailed rules for electronic signatures and competent service providers are set out in Act XXXV of 2001 on Electronic Signatures (E-Signature Act) which implements Directive 1999/93/EC on electronic signatures. If an electronic copy is made of hard copy documents in the manner prescribed by law, the electronic copy is equivalent to the original. Invoices issued with "EDI" or an advanced electronic signature and time stamp are as acceptable as hard copy invoices.

E-Communications Act Directive 2006/24/EC has been implemented in Act C of 2003 on Electronic Communications (E-Communications Act), effective from 15 March 2008. Hungarian communications providers are obliged to retain communications data for one year and, in case of unsuccessful call attempts, for six months.

The E-Communications Act lists each electronic communications service (such as fixed telephone and mobile telephone services, internet access, internet telephone, internet mail services and pre-paid anonymous mobile telephone services) and sets out in detail the data to be retained in connection with such services. The most important data to be retained, as applicable, are as follows:

— the subscriber's name and address and place and date of birth (if the subscriber is a natural person), the subscriber's company number or other registration number (if the subscriber is a legal entity), and the subscriber's bank account number – this is also applicable in the case of unsuccessful call attempts;

— the telephone number allocated to the terminal equipment of the user or subscriber or to the subscriber access point, or the user ID or any technical identifier;

— the location where the terminal equipment of the user or subscriber or the subscriber access point is installed, and the type of equipment;

— International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI);

— cell IDs;

— the date and time of the log-in and log-off by the subscriber, together with the IP address allocated to the communication; and

— date, time and duration of a communication.

A petition was submitted to the Hungarian Constitutional Court regarding the unconstitutionality of such newly implemented provisions, on the basis that the obligation to retain data violates the protection of personal data and or an individual's right to privacy. The Constitutional Court has not yet reviewed this petition and the newly implemented provisions remain in force.

Data Protection Act Data retention is classed as a type of personal data processing under the Hungarian Data Protection Act (any operation or set of operations that is performed upon personal data, whether or not by automatic means, including the collection, storage and use of such data). In practice this means that the retention of personal data, like any other type of personal data processing, requires the prior consent of the data subject in order to process their personal data. The Data Protection Act defines personal data as any information relating to an identified or identifiable natural person and any reference drawn, whether directly or indirectly, from such information. In the course of data processing, such information is treated as personal data as long as the data subject remains identifiable from this data. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Accounting Act and Tax Procedure Act There is no separate regime for electronic archiving of tax related documents in particular. Nonetheless, there are some specialised provisions dealing with particular aspects of e-archiving for tax purposes, such as the proper storage of electronic invoices. The primary framework of storage of tax related documents in general is provided by Act C of 2000 on Accounting (Accounting Act) and by Act XCII of 2003 on Tax Procedures (Tax Procedure Act).

In addition, a number of other laws and regulations (including guidelines of the Hungarian tax authority) contain certain specialised provisions. Generally speaking, those documents that may be issued electronically (e.g. electronic invoices) may also be stored electronically. However, the electronic data must remain safe from intentional or unintentional alterations, modifications or loss, or unauthorised access. Further, the tax authority must be able to gain access to these documents if required, i.e. usually in the case of a tax audit procedure. Taxpayers may of course hire specialised service providers to help them to comply with these rules.

Is there a legal definition of electronic archiving?

There is no strict legal definition of electronic archiving in Hungarian law. In addition to the requirements under the Data Protection Act for the retention of personal data, the E-Signature Act defines the scope of electronic archiving services (considered as part of electronic signature services). A key element of electronic archiving services is related to what is known as the "validity chain". This consists of the electronic document (or its image file) and the series of related information verifying that the advanced electronic signature or qualifying electronic signature and the time stamp affixed to the electronic document, as well as the certificate pertaining to them, were legally valid at the time the signature was executed and the time stamp was affixed.

The related information may include certificates, information linked to certificates, signature-verification-data, information pertaining to the current status of certificates, the electronic signature verification data of the certification-service-provider and information concerning the revocation of the certificate. When providing electronic archiving services, the archiving service provider must:

— archive the validity chain existing at the time of archiving to ensure that the documents are properly stored and cannot be disclaimed;

— ensure that the validity chain is not compromised so that the validity of electronic signatures it represents can be controlled in the long term;

— deliver the validity chain to the recipient as and when requested;

— supply a certificate upon request concerning archived electronic documents executed with electronic signatures or validity chains.

(Article 2 E-Archiving Decree Article 2 and 6(4) E-Signature Act)

For accounting purposes, which records must be kept by corporations and for how long?

Based on general accounting rules, invoices must be retained for a minimum of eight years and must be legible and accessible by a code of reference kept in the bookkeeping records. The annual report and supporting inventory, valuation, ledger statement, general ledger and other registers must be retained for a minimum of ten years (Articles 169 (1)–(2) and (5)–(6) of Act C of 2000 on Accounting (Accounting Act)).

For tax purposes, which records must be kept by corporations and for how long?

Tax requirements for the retention of records are the same as accounting requirements: invoices must be retained for a minimum of eight years and must be legible and accessible by a code of reference kept in the bookkeeping records. The annual report and supporting inventory, valuation, ledger statement, general ledger and other registers must be retained for a minimum of ten years. (Articles 169 (1)–(2) and (5)–(6) of Act C of 2000 on Accounting (Accounting Act)).

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Council Directive 2006/112/EC of 28 November 2006 amending Council Directive 77/388/EC has been implemented in Hungary by the Act on Value Added Tax and the Decree of the Finance Minister No. 46/2007 (XII.29.) PM on electronic invoice procedures and measures that include the verification of the origin and accuracy of invoices.

For VAT purposes, two methods of electronic invoicing may be used. One is to issue an electronic invoice, verifying it with an advanced electronic signature *(fokozott biztonságú elektronikus aláírás)* and a time stamp (issued by a qualified service provider). In this case, the data is to be stored in the same format as it was issued (i.e. electronically, which means that storing the print-outs only is not acceptable). However, in the event of a tax audit, the taxpayer must be able to present this data to the tax authority in one of the following formats: (i) .TXT, (ii) print-format or (iii) .XML format, either on a CD or floppy disk.

Another way to issue electronic invoices is through an electronic data interchange (EDI) system. This would usually be the case between business partners that issue significant numbers of invoices to each other. These invoices should be sent guaranteeing the authenticity and integrity of the contents and must be stored by the sender in the format transmitted and by the recipient in the format received. In addition, the issuer of EDI invoices should, at the end of each month, send to the purchaser a consolidated report of all the invoices that had been issued in the previous month. This report should also be stored by the purchaser.

Generally, senders and recipients must ensure that records of both electronic and EDI invoices are readily accessible and capable of being reproduced in a readable format, and that the systems preclude the possibility of any alterations of the data following issue of the invoice.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

The validity of an electronic signature or document cannot be disputed solely on the basis that the signature or the document only exists electronically. However, electronic documents cannot be used in family or inheritance law matters.

Electronic invoices have the same evidential value as hard copy invoices, provided that all the requirements with regard to their issuance, storage, signature and time stamp (as specified above) are fully complied with. In particular, the system for storing electronic invoices should enable both the invoice issuer and the supply in respect of which the invoice was issued, to be identified, whilst protecting the data contained in the invoice and ensuring its readability and accessibility. Printouts of electronic invoices do not have the same evidential value as the original electronic invoices.

Generally, documents issued non-electronically cannot be stored electronically. However, Article 169(6) of the Accounting Act provides an exception for accounting documents, provided they meet the electronic archiving criteria set out in the E-Archiving Decree, ensuring that the documents are readable and accessible and no subsequent modification has been made to them. However, the electronic format cannot replace the non-electronic original; both should be kept.

How long must documents be stored to cover the most important statutory limitation periods?

The Data Protection Act provides that personal data may only be processed to the extent and for the duration necessary to achieve the purpose of the processing. All documents containing personal data must be destroyed when no further legitimate grounds for processing such data can be established, unless the data subject has authorised the further storage/recording of their data or such authorisation is otherwise permitted by Hungarian law (Article 14 of the Data Protection Act). Given the general nature of the provisions of the Data Protection Act regarding the storage of documents containing personal data and the fact that specific retention periods are not stipulated, such documents are usually stored for the applicable limitation periods.

The general limitation period for civil law claims is five years. Claims relating to employment lapse after three years. A number of circumstances make it difficult to establish the date on which the statutory limitation period expires (e.g. the limitation may lapse, restart or be extended depending on the applicable law) and several claims have specific limitation periods. Therefore, minimum document retention periods should be considered on a case-by-case basis, depending on the nature of the particular documents.

For accounting purposes, invoices must be retained for a minimum of eight years and must be legible and accessible by a code of reference kept in bookkeeping records. The annual report and supporting inventory, valuation, ledger statement, general ledger and other registers must be retained for a minimum of ten years (Articles 196 (1)–2) and (5)–(6) Accounting Act).

Electronic and personal data relevant to an electronic signature certificate must be stored for at least ten years following expiry of the certificate's validity or until the resolution of any dispute concerning the electronic document (Article. 9(7) E-Signature Act).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Under Hungarian law, only certain corporate documents must be stored on company premises. Act IV of 2006 on Business Associations (Companies Act) states that the mandatory collection of the resolutions of the shareholders *(határozatok könyve)* of a Hungarian limited liability company (Kft.) must be kept at the Kft's registered office. Members may deviate from this rule in the company's Articles of Association. The Companies Act does not

differentiate between paper-based and electronic documents. The place of storage for non-personal information must satisfy general data security standards, similar to those required for the storage of personal information.

The taxpayer is under an obligation to keep invoices and other tax-related documents during the official limitation period (formally five years). The place of storage must be declared to the tax authority if the place where official documents are kept is not the same as the taxpayer's registered office or residence. This can be any place, but must be suitably accessible to the taxpayer to be able to present the documents upon request within three working days.

With regard to personal information, data protection requirements apply to both the storage of electronic copies and hard copy documents. Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest (Data Protection Act) regulates the processing (including storage) of electronic copies of documents if they contain personal data and such personal data processing takes place in Hungary. The Data Protection Act implements Directive 95/46/EC.

Personal data may be processed if the data subject has given his/her consent or if such processing is permitted by an act or decree of a municipality (the issuance of which is authorised by law). The data subject must be clearly and fully informed of all aspects of the processing of his/her personal data.

The transfer of data within the European Economic Area is treated in the same way as a transfer within the territory of the Republic of Hungary. Personal data may be transferred to data centres outside the EEA if:

— the data subject has given his/her consent; or

— the transfer is permitted by law and the laws of the country in question offer an adequate level of protection with respect to the processing of the personal data transferred.

An adequate level of protection for personal data is deemed to exist if:

— the European Commission has determined that the country in question ensures an adequate level of protection;

— there is a treaty between the country and the Republic of Hungary containing guarantees for the level of protection of personal data and the rights of data subjects as set out in the Data Protection Act; or

— the recipient data processor offers appropriate safeguards to ensure an adequate level of protection in the course of data processing (e.g. by way of data transfer agreement).

Must special measures be taken to ensure data security?

Under the general provisions of the Hungarian Data Protection Act, both personal and non-personal data must be protected against unauthorised access, alteration, transfer, disclosure by transmission or deletion as well as damage and accidental destruction and, in the case of electronic archiving, in accordance with the criteria listed above as prescribed by the E-Archiving Decree.

In the case of "EDI" invoices (i.e. invoices issued through an electronic data interchange system), the parties to the invoice are obliged to treat non-personal and personal information as confidential and ensure that it is not made available to unauthorised persons.

For the protection of personal data, the data controller, processor or electronic network operator must adopt special security measures, particularly where individuals' personal data is to be transferred electronically. The Data Protection Act does not set out these technical and organisational measures. When assessing such measures, the Hungarian Data Protection Supervisory Authority (DPA) considers the procedures affecting the exercise of access rights, logging of data requests and the registration of data processing.

Must special measures be taken to protect the data subjects' privacy?

The Data Protection Act does not specify the special measures that must be taken to protect the data subjects' privacy but contains certain general principles to follow in this respect. Data controllers and persons acting under the authority of the data controller must implement adequate safeguards and appropriate technical and organisational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of the Data Protection Act and other regulations concerning the confidentiality and security of data processing.

Data must be protected against unauthorised access, alteration, transfer, disclosure by transmission or deletion as well as damage and accidental destruction. For the technical protection of personal data, the data processor, any third party acting on its behalf, or the operator of telecommunications or information technology equipment must implement specific security measures where the processing involves the transmission of data over a network or via any other means of information technology. (Article 10 of the Data Protection Act).

The Data Protection Act does not specify the technical and organisational measures that must be taken to protect personal data. The publicly available investigations carried out by the DPA provide further guidance for assessing the appropriateness of the technical and organisational measures that should be taken. When reviewing such measures taken by data controllers, the DPA is checking, in particular, the procedures governing access rights, the logging of data requests and the registration of data processing.

The data processing principles under the Data Protection Act of particular relevance to archiving are that personal data must be:

(a) processed fairly and lawfully;

(b) accurate, complete and, where necessary, kept up to date;

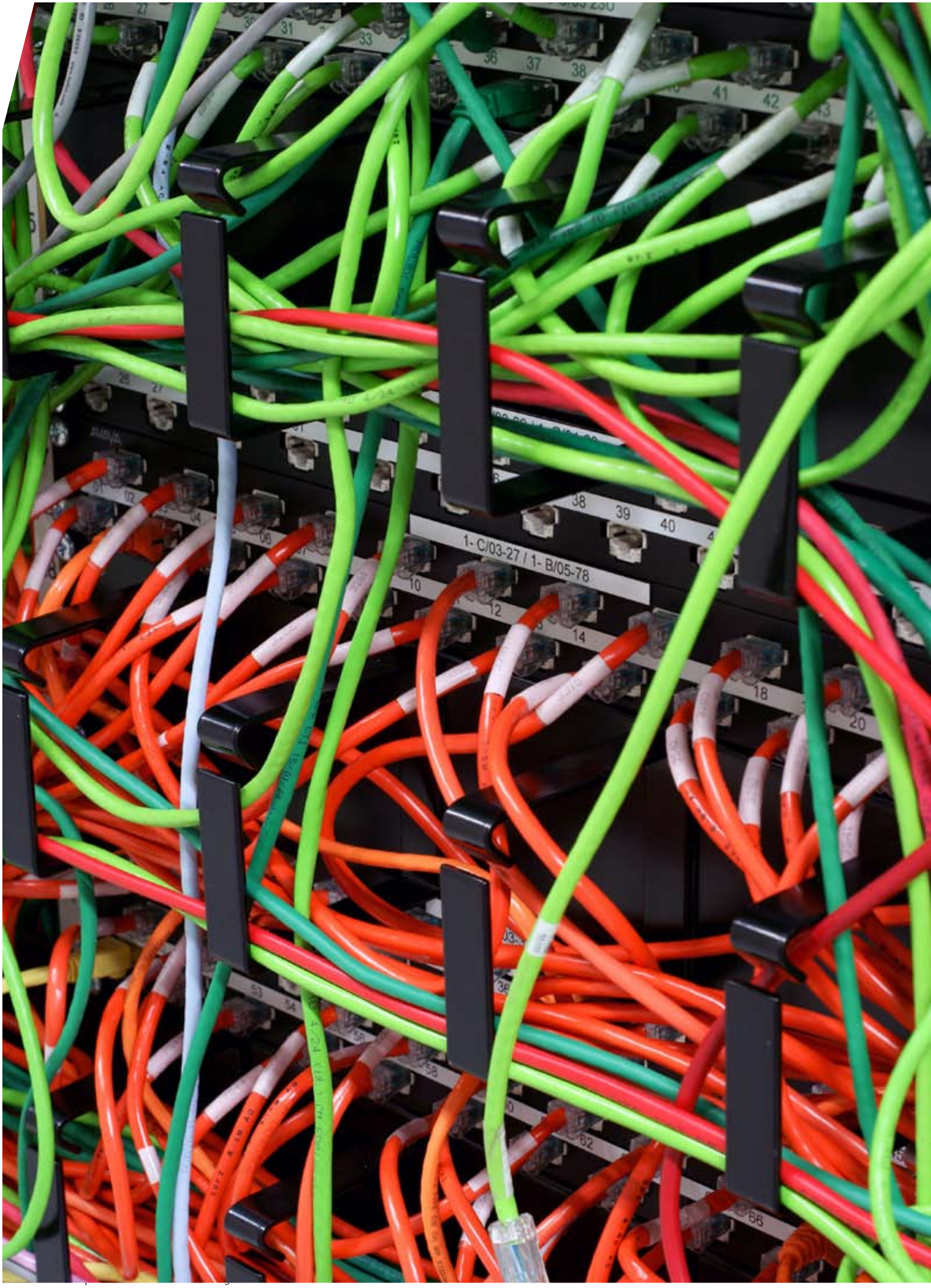
(c) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected; and

(d) only transferred outside the EEA if such transfer is in compliance with certain restrictions (as outlined above).

The Data Protection Act sets forth a special category of data (sensitive personal data): personal data revealing an individual's racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership, and personal data concerning an individual's health, addictions, sex life, or criminal record. Where sensitive personal data is being processed, the prior written consent of the data subject is required. Consent to the data processing can be given orally, in writing or by implication. Whilst the Data Protection Act requires written consent only for sensitive personal data, the data subject should provide consent in writing to enable the data controller or data processor to prove (in the case of any ambiguity) that such consent has been provided properly and lawfully. The practical interpretation of the "written" form is flexible; the click by the data subject on an "acceptance button" contained on electronic data collection forms is deemed to be sufficient written consent (Articles 2 and 3 of the Data Protection Act).

Anonymisation is required where personal data is used for the purposes of scientific research (Article 32 (2) of the Data Protection Act). Anonymising personal data is also mandatory when ceasing to process personal data for direct marketing purposes, either automatically (when the purpose of the data processing has lapsed) or at the request of the data subject (Article 3 (4) of Act CXIX of 1995 on the Use of Name and Address Information for the purposes of Research and Direct Marketing).

In addition to the general data protection requirements set out in the Data Protection Act, the E-Signature Act contains specific provisions on privacy protection. Certificated service providers must not transfer personal data to third parties without the consent of the data subject (except in certain circumstances permitted by law, e.g. criminal investigations, where national security is a concern, proceedings before courts or public authorities) (Article 11 E-Signature Act).


1- C/03-27 / 1- B/05-78

Italy

Paolo Scarduelli, paolo.scarduelli@cms-aacs.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

The legal framework governing electronic archiving in Italy may be summarised as follows:

DPR 28.12.2000 n. 445 (Single Text on administrative documents) This gathers all the existing legislation on electronic documents and the electronic preservation of documents.

Legislative Decree n. 82 dated 07 March 2005 ("CAD" i.e. Code of the digital administration) This reorganises the existing legislation on electronic documents and substitutes and integrates the DPR 445/2000.

CNIPA Resolution (National Centre for Information Technology in the Public Administration) of 19 February 2004 n. 11 This sets out the technical rules for the reproduction and preservation of documents to guarantee the conformity of these documents with the originals.

Legislative Decree n. 196 dated 30 June 2003, the Code concerning the protection of personal data (i.e. Privacy Code) and Annex B. The Privacy Code applies to any individual or legal person, including public bodies, and determines the purpose and manner for processing personal data (any information from which a living individual or legal person may be identified). The Privacy Code applies to personal data processing (the collection, recording, organisation, storage and destruction of personal data). Information containing personal data must, therefore, be stored in compliance with the data protection requirements of the Privacy Code. Annex B to the Privacy Code sets out how personal data should be processed to protect the privacy of data subjects.

DPCM 13 January 2004 (Prime Minister Decree) This sets out technical rules for the realisation, transmission, storage, duplication, reproduction and validation of the electronic documents.

DPR 11 February 2005 n. 68 (PEC – Electronic Certified Mail)

CNIPA Resolution (National Centre for Information Technology in the Public Administration) of 17 February 2005 n. 4. This specifies rules for the acknowledgment and verification of the digital document

D.L. 29-11-2008 n. 185 art. 16-bis. This contains simplification measures for families and enterprises.

Legislative Decree n. 10 dated 23 January 2002 This implements Directive EC/99/93 on electronic signature into Italian law.

Legislative Decree n. 109 dated 30 May 2008 This implements Directive EC/2006/24 on the storage of general data or data used for the supply of electronic communication systems. With regard to Legislative Decree n. 109/2008, the following Resolutions of the Authority for the Protection of Personal Data, set out provisions relating to electronic archiving: Resolution dated 17 January 2008 on the implementation of specific measures to guarantee that the transmission of data is carried out in compliance with applicable laws; Resolution dated 24 July 2008 on telephone transmissions; and Resolution dated 29 April 2009 on extending the measures set out in the Resolution of 24 July 2008. Data controllers must adopt appropriate measures by 15 December 2009.

Law Decree n. 185 dated 29.11.2008 passed into Law n. 2 dated 28 January 2009 Article 16 sets out new provisions on the storage of accounting books through electronic means. However, with regard to the

"preservation" of such accounting books, the provisions of Article 3 of CNIPA Resolution n. 11/2004 apply.

Article 2215 bis of the Italian Civil Code (electronic documentation) was introduced by the above-mentioned Law Decree 185/2008.

ASSONIME Memorandum (Italian Association of Companies Limited by Shares) dated 20 April 2009 This sets out new provisions relating to the electronic storage of accounting books.

Tax provisions:
Directive EC/2001/115 sets out rules for the drafting, transmission and electronic storage of electronic invoices.

Decree of the Ministry of Economy and Finance dated 23 January 2004 sets out methods for the fulfilment of tax requirements relating to electronic documents. There is also a related interpretation Memorandum of the Income Tax Office n. 36/E dated 06/12/2006.

Legislative Decree n. 52 dated 20 February 2004 (Implementation of Directive EC/2001/115) This simplifies the invoicing methods on VAT: Art 21: electronic invoices; Art 39: electronic storage; Art 52: the storage of invoices outside Italy (subject to the condition that the documents are directly accessible electronically). There is also a related interpretation Memorandum of the Income Tax Office n. 45/E dated 19/10/2005.

Directive EC/2006/112 dated 28 November 2006 Article 217 sets out the definition of an electronic invoice; Articles 232 to 237 sets out provisions relating to the electronic transmission of invoices; Articles 244 to 248 set out specific obligations on the storage of invoices; Article 249 sets out the right of access to invoices stored electronically in another EU Member State.

Law n. 244 dated 24 December 2007 (i.e. the Finance Bill 2008) Article 1 Paragraphs 209 to 214 sets out the obligation to issue, transmit, store and preserve, solely by electronic means, invoices issued in relation to transactions with state public bodies.

Is there a legal definition of electronic archiving?

Italian law makes a distinction between the "archiving" and "preservation" of electronic documents. Where legislation refers to the "archiving" of documents, it is in fact referring to the "preservation" of such documents (Article 1 of Deliberation n. 42 dated 13 December 2001 AIPI, Deliberation dated 19 February 2004 CNIPA).

Electronic archiving is the process of storing electronic and digital documents, assigning each document a unique reference number for ease of retrieval. Electronic archiving is carried out before the document preservation process and it is not subject to any specific requirements (Article 1 of Deliberation n. 42 dated 13 December 2001 AIPA, Deliberation dated 19 February 2004 CNIPA).

The digital preservation of electronic documents is the process required by law for civil and tax purposes whereby electronic documents and their data are recorded in a suitable system and registered with a time and date stamp (Deliberation n. 42 dated 13 December 2001 AIPA, Deliberation dated 19 February 2004 CNIPA).

Until recently, it was necessary to preserve the "unique" analogical originals, using a public official or public notary to certify completion of the storage procedure with a digital signature and a definite time stamp, whilst for those "non unique" documents, it was sufficient that these formalities were undertaken by the person responsible for the storage, appointed by the holder of the document.

Nowadays, pursuant to the Legislative Decree of 28 November 2008, the certification by public official/ notary is not always required for the digital preservation of "unique" analogical originals.

The Legislative Decree of 28 November 2008 provides that a special kind of "unique" analogical original document could still require certification by the public official/notary. These cases will be listed in future and special Decrees to be passed *ad hoc* by the Government.

Analogical documents, which must be kept by law, can be destroyed only after completion of the above-mentioned digital preservation procedure.

The laws currently in force provide for the appointment of a person responsible for the conservation process, with specific powers and obligations set by law, as well as the faculty for this person to delegate, in whole or in part, his duties to others, including third parties (through an outsourcing contract). Such person must work with the data protection officer, as provided in the Italian Privacy Code.

Pursuant to applicable laws, an electronic document can be considered to have the same value as a hard copy document if:

— it takes the form of a non-modifiable and static document;

— it is issued, in order to verify its date, originality and integrity, with a date and time stamp and an electronic signature;

— it is possible to display the document and to make it available, upon request, in hard copy and electronic format and when requested in the event of checks, controls and inspections;

— it can be recorded in a format enabling it to be read for years to come.

Italian law distinguishes between electronic and analogical documents and between the processes for the electronic storage of such documents.

As regards analogical documents, Memorandum 36/E sets out the difference between "unique" and "non-unique" original documents: "unique" original analogical documents are those documents the content of which cannot be obtained from other documents that must be kept by law (e.g. cheques or drafts). The books indicated in Article 2214 of the Italian Civil Code, invoices, etc., are "not unique" original analogical documents.

For accounting purposes, which records must be kept by corporations and for how long?

Any entity operating for business purposes must keep a ledger recording the date of the business's transactions and an inventory book of the business's profits and losses for the year, as well as all necessary accounting documents (determined by the nature and size of the business), invoices and client correspondence (Article 2214 and subsequent Articles of the Italian Civil Code).

The D.L.185/2008 introduced Article 2215-bis of the Italian Civil Code on the electronic storage of accounting books and documents, which sets out two requirements: the so called *"marca temporale"* (date and hour) and the digital signature of the entrepreneur (i.e. director's signature) or that of his delegate, to be recorded every three months. The electronic evidence of the date and time of the digital signature are electronically associated with the stored documents using a specific program.

Furthermore, the above-mentioned law introduced the option of keeping the payroll and employment ledger *(Libro Unico del Lavoro)* electronically.

Accounting documents, invoices, letters and related copies must be kept for ten years from the date of last filing. These documents may be preserved through electronic registration. (Article 2220 of the Italian Civil Code; Article 16 of Law Decree 29 November 2008 n. 185).

For tax purposes, which records must be kept by corporations and for how long?

Under the Italian Civil Code and tax laws, mandatory accounting documents must be kept for tax reasons until the inspection period has expired for the relevant fiscal period (Article 22 Decree President of the Republic (DPR) n. 600 of 1973). In general, and for tax purposes, relevant documents must be kept for at least four years after submission of the relevant tax and VAT declaration (Articles 43 DPR 600/1973 and 57 DPR 633/1972).

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Directive 2001/115 has been implemented in Italy by Legislative Decree n. 52 of 2004, introducing the option of issuing invoices electronically.

An electronic invoice is considered issued when it is transmitted by electronic means (Article 21 of DPR633/1972 as amended by the above-mentioned Decree n. 52 of 2004; Memorandum n. 45/E of the Income Tax Office).

Article 39 DPR 633/1972, modified as a consequence of the implementation of the Directive, requires that registers, bulletins, files, invoices, customs bills and other relevant documents are kept pursuant to Article 22 DPR 600 dated 29 September 1973, or until the relevant accounting data are recorded in the books and registers as required by law. Electronic invoices transmitted or received electronically are stored in electronic format. Electronic invoices delivered or sent in hard copy format can also be stored electronically.

Memorandum 45/E issued by the Income Tax Office (i.e. *Agenzia delle Entrate*) interprets the above decree, specifying obligations where electronic invoices are used and, where such invoices are used, the obligation to keep registers and documents electronically. The decree also provides for inspection by the tax authorities of documents stored electronically.

The following changes set out in the Directive have been implemented:

— the option to issue and send invoices electronically;

— the option to issue electronic invoices even where the recipient is resident in a country which offers no mutual assistance;

— mandatory requirements concerning the content of the invoice;

— the option to issue, to the same client, a single invoice for separate activities made in the same day;

— the obligation to indicate in the invoice that the same invoice has been drafted by the client or by a third party on behalf of the assignor.

The use of electronic invoicing is permitted with the prior consent of the recipient.

Where an electronic invoice is issued, the signature and date and time of issue must be marked on the invoice. The storage of the electronic invoices pursuant to the above-mentioned preservation process must be made within 15 days of their receipt/issue.

Legislative Decree n. 52 of 2004 has introduced the principle of uniformity for "type of documents": if receipt of electronic invoices is permitted for one supplier, it becomes mandatory to store electronically all the invoices (including those received in hard copy).

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Accounting procedures carried out through electronic means (i.e. electronic filings) are equivalent to those carried out non-electronically (i.e. paper filings) and have the same legal validity, provided that:

— the requirements set out in the Italian Civil Code on the progressive numbering of pages and order of accounts are met;

— a qualifying electronic signature (i.e. digital signature) is used;

— there is electronic evidence of the date and time of the storage/issue/receipt of the document (*"marca temporale"*);

— the documents can be easily viewed and printed.

With regard to insurance contracts/registers and the digital preservation process, Regulation n. 27 of 2008 issued by the Italian insurance regulator (ISVAP), formally endorses

the validity of registers and insurance documents that are kept digitally. The digital preservation of original hard copy registers must be carried out in accordance with the provisions on the preservation of original documents at the end of each quarter. In such cases, the digital documents should have the same evidential value of the hard copy originals.

Businesses must keep insurance registers for ten years (Article 2220 Italian Civil Code) except for register entries relating to life insurance contracts that must be kept for 20 years from the date of the last entry.

How long must documents be stored to cover the most important statutory limitation periods?

Accounting documents, invoices, letters and related copies must be kept for ten years from the date of last filing. Under the Italian Civil Code and tax laws, mandatory accounting documents must be kept for tax reasons until the inspection period has expired for the relevant fiscal period (Article 22 Decree President of the Republic (DPR) n. 600 of 1973). In general, and for tax purposes, relevant documents must be kept for at least four years after submission of the relevant tax and VAT declaration (Articles 43 DPR 600/1973 and 57 DPR 633/1972).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Documents in electronic format may be stored at the premises of the company or at the premises of a third party (outsourced provider). These providers (public or private) must adhere to the legal requirements of the "substitutive document preservation procedure" and the location of the server and name of the company carrying out document preservation must be notified to the Income Tax office.

Electronic invoices may be archived abroad provided that mutual assistance with that country is available and adequate guarantees are given by the parties involved (Article 39 DPR 633/1972 (modified by Legislative Decree 52/2004). EU countries should have executed mutual assistance agreements with Italy with regard to tax matters, and therefore in such countries the data could be electronically stored.

The body resident in the foreign territory must ensure (for inspection purposes) computerised access to the data archive and that all archived documents and data, including certificates necessary to guarantee the originality and integrity of electronic invoices (as set out in Article 21(3)), are printable and transferable to other systems.

There is currently no provision in Italian law which expressly permits the storage abroad of accounting documents and books held electronically. Despite certain commentators suggesting such storage could be possible provided preservation of the accounting documents is guaranteed, this practice is not accepted by the Income Tax Office.

Must special measures be taken to ensure data security?

Pursuant to the Personal Data Protection Code (Art. 29), the data controller may designate one or more data processors. Where designated, the data processor shall be selected among entities that can appropriately ensure, on account of their experience, capabilities and reliability, thorough compliance with the provisions in force applying to processing as also related to security matters.
If necessary, on account of organisational requirements, several entities may be designated as data processors also by subcontracting the relevant data processing tasks. The tasks given to the data processor are detailed in writing by the data controller. The data processor must abide by the instructions given by the data controller in carrying out the processing. The data controller must supervise the data processors) to ensure compliance with instructions and the provisions referred to in Paragraph 2, also by means of regular controls.

Broadly speaking, the party responsible for document preservation has certain obligations in relation to planning, monitoring, documentation control, protection and security measures.

If documents preserved electronically contain personal data, the party responsible for preservation must ensure compliance with the security measures set out in Articles 31 to 36 of Decree n. 196 dated 30 June 2003 and Annex B to the Decree. Whenever the relevant party engages in activities involving the processing of personal data, the prior consent of the data subject must be obtained (verbal consent is acceptable provided it is not tacit or presumed).

The processing of personal data stored electronically is only permitted if the following standards, as specified in Annex B, are met:

— there is an electronic authentication (e.g. procedures for the verification of passwords);

— authentication credentials are adopted (e.g. identification codes and related procedures for their non disclosure/access);

— an authorisation system is used;

— there are periodic updates of the subjects appointed and in charge for the management or maintenance of the electronic instruments;

— electronic documents and data are protected against unlawful access and use;

— procedures are adopted to protect against data loss or destruction, including data and system recovery procedures;

— a document detailing security measures is updated on a yearly basis (i.e. *Documento Programmatico sulla Sicurezza*);

— coding techniques or identification codes are used for the processing of certain sensitive personal data (such as health and sexual orientation information) by healthcare professionals.

The party carrying out document preservation is responsible for ensuring compliance with applicable laws and may face criminal sanctions for infringement of privacy laws (Article 167 Privacy Code on the crime of unlawful processing of personal data and Article 169 Privacy Code on the crime of failing to adopt minimum safety measures to protect data).

Must special measures be taken to protect the data subjects' privacy?

Annex B to the Privacy Code (the "Code") sets out how personal data should be processed to protect the privacy of data subjects.

In particular, it should be noted that:

— Personal data may be stored for a time not exceeding the period required for the purposes for which the data has been collected and is processed. Retaining personal data beyond this time increases the risk of it being destroyed, lost or accessed by unauthorised parties. The Privacy Code sets out this general principle and other specific data retention restrictions. For example, Art. 123 provides that data relating to communication services (public communication networks or electronic mail services) may only be stored for invoicing purposes or possible consequent complaints, and not beyond a period of six months. A longer period may be permitted only in cases of judicial claims.

— The Code requires the adoption of various security measures to ensure that the data processed are stored and controlled according to minimum security measures. The security measures taken must be reported on an annual "Programmatic Document on Security" (DPS), which must be updated every year by 31 March. The DPS must contain measures including:

— identification of the personnel authorised to have access to the data;

— periodical change of passwords;

— risk analysis for the kind of data collected;

— periodical data back-up;

— measures of encryption of the personal data;

— measures for the destruction of data archives.

Pursuant to Art. 11 of the Code on Personal Data, personal data must be:

— processed lawfully and correctly;

— collected and stored for specific, explicit and legitimate purposes and used in other processing operations in a manner compatible with these purposes;

— accurate and updated when necessary;

— relevant, complete and not disproportionate in relation to the purposes for which it is collected or subsequently processed;

— stored in a form which identifies the data subject for a period not exceeding the time necessary for the purposes for which the data has been collected and is processed.

Personal data processed in violation of the law relating to the processing of personal data, may not be used.

Sensitive personal data is personal data relating to an individual's racial and ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, unions, associations or organisations of a religious, philosophical, political nature, or trade union membership, and personal data able to reveal the state of health and sex life of an individual. Such data may only be processed with the consent of the data subject and if expressly authorised by the Data Protection Supervisor (Art. 26 Italian Privacy Code). The Supervisor must notify its decision within 45 days from such request, and if he does not notify any decision within this period, the request is deemed rejected. In giving such authorisation, or even after giving such authorisation, the Supervisor may prescribe measures and arrangements to guarantee the protection of data subjects' privacy rights.

The Supervisor's authorisation is not required:

— for data about members of religious entities or data subjects who have contacts with the same entities only for religious purposes;

— for data concerning membership to associations or trade unions or categories, or other associations;

— the consent of the sensitive personal data subject is not required:

— in the case of data processing carried out by associations or non-profit entities with political, philosophical, religious or trade intent, used for legitimate purposes as set out in the certificate of incorporation, company by-laws or collective agreements;

— when processing sensitive personal data is necessary for the protection of the life of third parties. In the case of protecting the life of the data subject, if he is not able to give his consent, such consent can be given by those who have parental right to decide;

— in the case of data processing necessary for carrying out investigations to claim or defend a right in court, provided that the data is used exclusively for this purpose and only for the period of time necessary and that the right at issue has the same importance as the sensitive personal data being processed.

— when sensitive personal data processing is necessary to fulfil specific obligations or duties required by law.

Data capable of revealing an individual's state of health cannot be disclosed.

The Netherlands

Wouter Seinen, wouter.seinen@cms-dsb.com
Silvia Corine van Schaik, silvia.vanschaik@cms-dsb.com
Gilbert Joskin, gilbert.joskin@cms-dsb.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

There is no general law or legal framework regulating electronic archiving in the Netherlands. Electronic archiving requirements are set out in various specific laws including the Personal Data Protection Act (*Wet bescherming persoonsgegevens*), tax laws and laws relating to specific (criminal) records held by the Dutch government.

Personal Data Protection Act (PDPA) The PDPA applies to all companies and persons that have control over the processing of personal data. Personal data must be retained in accordance with the requirements of the PDPA. Therefore, personal data may not be kept for longer than is necessary for the purposes for which it is processed (Article 10 PDPA).

Laws relating to government-held records There are specific laws that provide a legal basis to and regulate certain records held by the Dutch government, such as the law in respect of criminal records, the municipal personal records database and social security.

The EC Data Retention Directive The EC Data Retention Directive has not yet been implemented in the Netherlands. The Government has prepared a bill implementing the Directive and this bill is currently before the Dutch Parliament. The proposal provides for the Directive to be implemented in:

— the Telecommunications Act *(Telecommunicatiewet)*;

— the Personal Data Protection Act;

— the Code of Criminal Procedure *(Wetboek van Strafvordering)*;

— the Criminal Code *(Wetboek van Strafrecht)*; and the Economic Offences Act *(Wet op de economische delicten)*.

The proposal provides for a data retention period of six months.

Is there a legal definition of electronic archiving?

There is no strict legal definition of electronic archiving in Dutch law.

If personal data is being archived electronically, the PDPA will apply, as this is classed as the processing of personal data contained in a relevant filing system.

The PDPA defines the processing of personal data as every activity carried out in respect of personal data, including (inter alia) the storage of such data. The PDPA only applies if the processing of personal data is (partly) automated or if the data processed are contained or are intended to be contained in a filing system. On this basis, electronic archiving falls within the PDPA definition.

Personal data is defined as any information relating to an identified or identifiable natural person. A person is considered identifiable if the information (alone or in combination with other information) is so characteristic of a person that he or she can be identified on the basis of that information. This includes information that can only indirectly identify a person, including any information that does not include a person's name (or other directly identifying information such as a date of birth or an address), but when combined with other information is capable of identifying a person. Under Dutch law, the broad definition of personal data means that information is easily classed as personal data. For example, the Dutch Data Protection Authority classes an IP-address as personal

data, the processing of which therefore falls under the PDPA.

For accounting purposes, which records must be kept by corporations and for how long?

The accounting obligations of corporations (and other legal entities) are set out in Article 2:10 of the Civil Code *(Burgerlijk Wetboek)*.

The board of a corporation must keep account of records of:

— the financial condition of the corporation;

— the corporation's activities, in accordance with the requirements arising from these activities.

Books, records and other data carriers must be kept in such a way that the associated rights and obligations may be assessed at any time. The information may be archived electronically (Article 2:10(4) Civil Code).

In addition, the board must keep a written record of the balance sheet and a statement of income and expenditure for the previous financial year. These documents may not be archived electronically without retaining the hard copies.

The board is under an obligation to maintain the above records, books, balance sheets and other data carriers for a period of seven years.

For tax purposes, which records must be kept by corporations and for how long?

Article 52 of the State Tax Act *(Algemene Wet inzake Rijksbelastingen)* states that books, records and other data carriers must, for tax purposes, be kept for at least seven years.

Corporations must keep books, records and other data carriers concerning their financial position and their company, profession or activities, in such a way that rights, obligations and data relevant to calculating and levying taxes can be determined at any time.

Such data may be stored digitally (Article 52(5) State Tax Act) except for balance sheets which must be maintained in hard copy format.

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

The general rules of Articles 2:10 Civil Code, 52(4) State Tax Act and more specifically, Article 31(6) Turnover Tax Decree 1968 (*Uitvoeringsbeschikking Omzetbelasting* 1968), apply to the electronic storage of invoices and require the retention of invoices for seven years.

For administration related to real estate, the retention period for invoices is nine years (Article 34a Turnover Tax Act 1968).

Directive 2001/115/EC has been implemented by amendment to the Turnover Tax Act 1968 (*Wet op de omzetbelasting* 1968). Article 35c sets out the rules for the storage of incoming and outgoing invoices. However, it does not specify a retention period for invoices. Where invoices are sent or received electronically, electronic storage is permitted, provided that the authenticity, integrity and readability of the content of the invoice are guaranteed throughout the retention period. Data that verifies the authenticity of the invoice and the integrity of the content must also be stored.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Electronic copies of invoices and contracts do not have the same evidential value as paper documents.

Unlike an electronic copy of a document, an original signed hard copy document is considered to be compelling proof that constitutes valid evidence by virtue of law (Articles 156, 157 and 160 Code of Civil Procedure *(Wetboek van Burgerlijke Rechtsvordering)*). The evidential value of an electronic copy of a contract is determined at the court's discretion (Article 149 Code of Civil Procedure). Digital contracts that meet the requirements of Article 6:227a Civil Code and are signed using a digital signature satisfying the requirements of Article 3:15a Civil Code (implementing Directive 1999/93/EC) do have the same evidential value as hard copy contracts.

Some legal actions (such as the assignment of copyright or a non-competition clause in employment contracts) must be executed by deed *(akte)* to have legal effect. Such a deed may be executed traditionally (by signed hard copy) or electronically, provided the electronic deed satisfies the requirements of Articles 6:227a and 3:15a Civil Code.

Electronic invoices will be accepted as evidence by the tax authority provided that the authenticity and the integrity of the content of the invoice is guaranteed by (i) an advanced digital signature (as defined in Article 2 (2) of Directive 1999/93/EC); (ii) Electronic Data Interchange (as defined in Article 2 of EC Recommendation nr. 1994/820/EC; or (iii) another method which is reported to the tax authority (Art. 35b Turnover Tax Act 1968), for example, sending invoices by e-mail or making invoices available to the customer online. It is important to note, however, that customers are under no obligation to accept electronic invoices.

How long must documents be stored to cover the most important statutory limitation periods?

Dutch law provides for many different limitation periods for different kinds of actions. For the most common civil actions (such as claiming performance of an agreement, payment, or compensation of damages) the law provides for a limitation period of five years (Article 3:307 *et seq.* Civil Code).

Claims based on pollution, dangerous substances and mining activities have an extended limitation period of 30 years (Article 3:310(2) Civil Code).

In the exceptional situation where the law does not provide for a specific limitation period, rights of action are prescribed on the expiry of 20 years (Article 3:306 Civil Code).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Non-personal information There is no general obligation in Dutch law to store electronic copies of documents at either the company premises or within the EU. Provided archived documents remain "available", corporations may store them anywhere.

Personal information Electronic documents containing personal data may be transferred to and stored in any EEA country. Transferring personal data outside the EEA is only permitted when the respective country or the recipient maintains an adequate level of data protection (e.g. the safe harbour programme for recipients based in the USA) or when one of the exceptions of Article 77 PDPA applies.

Tax There is no general provision in Dutch law requiring electronic copies of documents to be stored at either the company premises or within the EU, provided information can be made available to the tax authority within a reasonable period of time. Furthermore, Article 35c (2) Turnover Tax Act 1968 (implementing Directive 2001/115/EC) provides that if invoices are sent or received electronically and stored in another EU country so as to be accessible online, the tax authority has the right to access the invoices digitally and may download them for inspection purposes.

Must special measures be taken to ensure data security?

Non-personal information Dutch law does not contain a general provision setting out the special measures that must be taken to ensure the security of non-personal data. Nonetheless, it may be considered unlawful (f.i. under Article 6:162 Civil Code) not to exercise the due care (and diligence) that should be exercised. This includes failing to take measures to protect confidential information.

Personal data Electronic documents containing personal data must be protected by adequate technical and organisational measures (Article 13 PDPA). The extent to which such measures must be taken depends on the nature of the data being processed, the scale of processing activities, the risk of abuse of personal data and the state of technological development.

Must special measures be taken to protect the data subjects' privacy?

Aside from the Article 13 PDPA requirement to take measures to protect the personal data contained in electronic documents, Dutch law does not contain a provision that specifies the special measures that should be taken to protect data subjects' privacy. However, personal data may only be processed in compliance with the PDPA, which contains some general principles that may lead to an obligation to take special measures. For example, a data controller must process personal data with due care and may only process personal data to the extent that this is necessary and proportionate. The measures that will need to be taken to protect data subjects' privacy will depend on the nature of the personal data and the purpose for which it is to be processed. In general, a data controller is under an obligation to ensure that personal data is adequate, relevant, not excessive, accurate and kept up to date.

Furthermore, personal data may not be stored any longer than is necessary for the purpose for which it is collected and processed (Article 10 PDPA), unless it is stored for historic, statistic or scientific purposes and the data controller has taken measures to ensure that the data is only used for those purposes.

The law sometimes provides for a specific retention period in relation to certain types of data, for example, health care providers must store files relating to medical treatment for 15 years, unless it is necessary to store them longer (Article 6:454 Civil Code).

Where the law does not specify a specific retention period for a particular type of personal data, the data controller must decide how long such data may be stored. In some cases, archiving may be the purpose for which personal data are stored. In general, if personal data is anonymised (a process that requires complete anonymisation, as opposed to simply removing directly identifiable information), and is therefore no longer classed as personal data under the PDPA, the PDPA restriction on how long this data may be retained no longer applies.

Whilst personal data should not be stored for longer than necessary, the data controller is also prohibited from removing personal data from an archive too soon, as this may affect the data subject's right to access their data and to obtain information on the parties with whom this data has been shared. In its decision of 7 May 2009, the European Court of Justice held that a Dutch public entity had to store certain personal data for more than a year to be able to provide data subjects with information as to the recipients of such personal data held by the public entity.

The PDPA imposes stricter obligations on data controllers who process sensitive personal data (personal data relating to an individual's religion, beliefs, race, ethnic origin, political opinions, health, sexuality, trade-union membership, criminal records and illegal or objectionable behaviour, following the prohibition of such behaviour).

Sensitive personal data may only be processed if one of the exceptions in the PDPA applies (Article 16 *et seq.* PDPA). One such exception is that the data subject has given his or her explicit consent to the processing of such personal data (Article 23 PDPA). Whilst the PDPA does not specify measures that should be taken to protect sensitive personal data, the data controller is expected to take additional steps to protect sensitive personal data, including the implementation of enhanced security measures.

Poland

Dr. Agnieszka Besiekierska, agnieszka.besiekierska@cms-cmck.com
Dr. Andrzej Krasuski, andrzej.krasuski@cms-cmck.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

Polish Telecommunications Law (Ustawa prawo telekomunikacyjne (TL) The EC Data Retention Directive has been implemented in Polish Telecommunications Law (*Ustawa prawo telekomunikacyjne* (TL)). Under the Act amending the TL, all data stored in accordance with the EC Data Retention Directive must be retained for two years.

Polish law also provides a tax framework that regulates the electronic archiving of invoices. This is the Regulation of the Minister of Finance dated 14 July 2005 relating to issuing and sending, as well the storage of, electronic invoices, implementing Directive 2001/115/EC).

Polish Data Protection Act Under the Polish Data Protection Act of 29 August 1997 (Data Act), the electronic archiving of documents containing personal data constitutes the "processing" of personal data, as defined in the Data Act. Therefore, the electronic archiving of personal data is subject to the general rules regulating the processing of personal data. IT systems used for personal data archiving should comply with the Regulation of the Minister of Internal Affairs and Administration, dated 29 April 2004, on personal data processing documentation and the technical and organisational conditions that should be fulfilled by devices and computer systems used for processing personal data (Regulation).

The Data Act provides that personal data may only be processed (e.g. stored or archived) until the legitimate purpose for which the data were collected, has been fulfilled. Thereafter, such data should either be deleted or anonymised unless such data must be retained for a period and purpose otherwise prescribed by law, for example, the retention of certain employee records pursuant to Polish employment law.

Is there a legal definition of electronic archiving?

There is no strict legal definition of electronic archiving established in Polish law.

The electronic archiving of personal data falls within the Data Act definition of personal data "processing" (any operation which is performed in relation to personal data, including the collection, recording, storage, organisation, alteration, disclosure and erasure of such data, and in particular, operations performed in computer systems). Accordingly, the creation and/or maintenance of archives containing personal data (information relating to an identified or identifiable natural person) constitutes the processing of personal data. Personal data that has been anonymised and therefore cannot be connected with a particular person is classed as non-personal data and is not subject to the Data Act.

For accounting purposes, which records must be kept by corporations and for how long?

Documents describing accounting principles, account books, accounting documents, inventory records and financial statements must be appropriately stored and measures must be taken to protect these records from unauthorised modification, unauthorised disclosure, damage or destruction (Article 71 Paragraph 1 Accounting Act *(Ustawa o rachunkowości)*).

Approved financial statements must be stored permanently (Article 74 Paragraph 1 Accounting Act *(Ustawa o rachunkowości)*).

In addition, other documents should be stored for at least the following periods:

account books – five years;

— employee payroll sheets or equivalent documents – for a period as required under retirement, pension, or tax regulations, but not less than five years;

— accounting documents relating to retail sales income – until the date of approval of the financial statements for a given financial year, but not before the date when the persons entrusted to monitor inflow and outflow inventory has accounted for them;

— accounting documents concerning long-term investments, loans, claims under civil, criminal or tax law – five years starting from the year after the year in which the above events are completed, settled or prescribed respectively;

— documentation explaining the adopted accounting methods – at least five years following the date on which these accounting methods become redundant;

— documents relating to product warranties and complaints – one year after the expiry of the warranty or settlement;

— inventory documents – five years;

— other accounting documents – five years.

(Article 74 Paragraph 2 Accounting Act)

These periods run from the beginning of the year following the financial year to which the documents refer.

The Accounting Act provides that financial books may be stored electronically. However, from a practical point of view, especially for tax inspection purposes, they should also be kept in hard copy form.

In addition to the above Accounting Act requirements, the Act on Pensions from the Social Insurance Fund *(FUS)* provides that the insurance premium payer must retain employee remuneration information and pay slips for 50 years from the day the insured stopped working for the insurance premium payer.

For tax purposes, which records must be kept by corporations and for how long?

The Tax Ordinance *(Ordynacja Podatkowa)* requires that taxpayers shall keep all invoices they issue for five years following the year in which the tax payment deadline expires.

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Article 112 Value Added Tax Act *(Ustawa o podatku od towarów i usług)* requires taxpayers to keep all documents relating to the calculation of VAT until the tax obligation is prescribed, i.e. five years following the end of the year in which the tax payment deadline expired. Electronic storage of invoices must comply with several rules contained in the Regulation of the Minister of Finance, which was issued on 14 July 2005 to implement Directive 2001/115/EC.

The principal requirements regarding electronic archiving of invoices are as follows:

— the recipient of the invoices shall accept the issuing and sending of invoices in electronic form;

— the authenticity of the electronic invoices shall be guaranteed in one of the following ways: (i) use of a secure electronic signature or (ii) use of electronic data interchange (EDI), in accordance with an agreement based on the European model of data interchange, where the executed agreement sets out procedures guaranteeing the authenticity and integrity of the invoice;

— Polish tax authorities shall be guaranteed, on request, easy electronic access to the invoices and the ability to print them off;

— Polish tax authorities shall be informed where the invoices are stored;

— the invoices shall be kept in a manner which guarantees: (i) their authenticity and the integrity of their content and (ii) their legibility throughout the storage period;

— the correct invoices and duplicates of the invoices shall be kept in electronic form, if they relate to invoices issued and transferred in electronic form.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Electronic invoices have the same evidential value as paper documents if issued in accordance with secondary regulations on electronic invoices. Under these regulations, electronic invoices are equal to invoices issued in paper form in two situations. Firstly, where the integrity and authenticity of electronic invoices can be guaranteed by: (i) a secure electronic signature or (ii) an electronic data interchange (EDI), in accordance with an agreement based on the European model of data interchange, where the agreement sets out the procedures guaranteeing the authenticity and integrity of the invoice (EDI). Secondly, where the recipient of the invoice has given prior consent to issuing and sending electronic invoices. Such consent may be provided in written or electronic form (where consent is provided in electronic form, electronic signature or EDI requirements apply).

Electronic copies of contracts have the same evidential value as contracts in hard copy form, provided they are signed using a secure electronic signature verified by a valid qualifying certificate in accordance with the Act on Electronic Signatures of 18 September 2001.

How long must documents be stored to cover the most important statutory limitation periods?

There is no law governing how long documents should be stored in general. This depends on the type of documents to be stored.

With regard to contracts, it is important that they are kept for at least as long as the relevant limitation period for bringing legal action. For contracts, the limitation period is, in general, ten years after performance of the contract (or the date the contract should be performed) unless otherwise provided by law. For example, the statutory limitation period for civil law claims in respect of periodic services (e.g. rent for a lease, ground rent, tenancy rent) and in respect of conducting economic activity, is three years (under the Polish Civil Code *(Kodeks Cywilny)*.

The concept of economic activity is not defined in the Polish Civil Code. Therefore, there are many interpretations of this concept and it can be difficult to determine whether the three-year limitation period applies in a particular case. It is important to note, however, that the claim must be directly related to a business entity's economic activity.

The fact that it is the business entity that makes the claim or against whom the claim is made, is not sufficient.

More specific legal provisions apply to the storage of specialist documents, including tax documents, employment documents and corporate documents.

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Invoices issued or received in electronic form may be stored in another EU country on the condition that the relevant tax authority receives prior written notification of the storage location (Section 6.2 of the Regulation of the Minister of Finance of 14 July 2005). However, any change to the place of storage should be notified to the relevant tax authority within seven days of such change.
Copies of invoices issued or received in electronic form can be stored at the premises of the entity receiving the invoice, the premises of the entity issuing the invoice or at the premises of a third party data archiving service provider (including a data centre), provided the tax authorities are notified and the accessibility of these documents can be guaranteed.

Under the Accounting Act, accounting documents and inventory records can be kept at:

— the company's head office;

— branch offices;

— the premises of a third party data archiving service provider, as long as the tax authorities are notified of this and the accessibility of these documents for inspection purposes can be guaranteed.

Accounting books cannot be stored abroad.

Under the Data Act, companies are not obliged to process (e.g. store) personal data exclusively on their premises, and may outsource the storage of personal data to third parties. Use of third parties for the processing (including storage) of personal data requires that an agreement is entered into between the data controller and the third party, containing provisions required by the Data Act, including, at least, the scope and purpose of the data processing to be carried out by the third party service provider.

Processing (e.g. storage) of personal data may take place within the European Economic Area ("EEA") and outside the EEA, provided certain conditions are fulfilled.

As regards the EEA, aside from the requirements relating to the use of a third party service provider set out above, there are no specific requirements for the transfer of personal data to such third party if it is headquartered within the EEA.

Where personal data is to be stored in a non-EEA country, transfer of this data may take place only if the laws of the destination country ensure at least the same level of data protection as Polish law. This requirement does not apply in certain circumstances, which include:

— the data subject has given his/her written consent to the transfer outside the EEA;

— the transfer is necessary for the performance of a contract between the data subject and the data controller or takes place in response to the data subject's request,

— the transfer relates to personal data that is publicly available,

— the transfer is required by law or by the provisions of any ratified international agreement,

— the transfer is necessary for the performance of a contract concluded in the interests of the data subject between a company and another entity,

— the transfer is necessary in order to protect the vital interests of the data subject.

Where the data protection law of a non-EEA country to which personal data is to be transferred falls below the required standard, the prior consent of the Polish Data Protection Authority must be obtained and the data controller must ensure that adequate safeguards are put in place to protect the privacy, rights and freedoms of the data subject.

Must special measures be taken to ensure data security?

Account books, accounting documents, inventory records and financial statements must be stored appropriately to prevent unauthorised modifications, unauthorised disclosure, damage or destruction (Article 71.1 Accounting Act).

Where account books are computerised, data protection measures should be adopted, such as the use of damage resistant data carriers, appropriate external security measures and back-up for computer data files, provided these measures ensure the durability of accounting records for the same period of time required for account books, whilst ensuring the protection of computer software and computerised accounting records through the application of appropriate technical and organisational measures to protect against unauthorised access or destruction.

The party processing personal data must implement technical and organisational measures to protect this personal data, as appropriate to the risks associated with the data and the category of data being protected, in order to ensure protection of the data against unauthorised disclosure, access by unauthorised persons, processing in violation of the Data Act or any modification, loss, damage or destruction (Article 36 Data Act).

The Data Act itself does not provide an exhaustive list of measures that should be taken. The data processer should undertake appropriate assessment of how the personal data should be protected.

The Data Act contains a few organisational requirements relating to data processing, and stipulates that the party processing personal data should:

— maintain documentation describing the way in which the data was processed and measures taken to protect the data,

— appoint an administrator responsible for information security and supervising compliance with security principles,

— grant the appropriate authorisation to persons who are to process personal data. These authorised persons are obliged to ensure the confidentiality of the data and methods used to protect it,

— keep the list of persons authorised to process personal data,

— ensure supervision as regards: the data that has been entered into the data system, when this was carried out and by whom, and to whom it was transferred.

Additionally, Polish law contains specific regulations as to the minimum security requirements that must be fulfilled by IT systems used for personal data processing. These requirements are contained in the Regulation of the Minister of Internal Affairs and Administration, dated 29 April 2004) regarding personal data processing documentation and the technical and organisational requirements that should be fulfilled by data carrying devices and computer systems used for processing of personal data.

Must special measures be taken to protect the data subjects' privacy?

The conditions for personal data processing (set out above) are aimed at ensuring data subjects' privacy. The Data Act also sets out other rules and principles, for example:

— personal data collected and processed by a data controller must be adequate for the purpose for which it is to be processed. Any processing of data that exceeds the purpose of such processing may be considered unlawful by the Polish Data Protection Authority, even where the data subject has given his/her consent;

— data subjects have extensive rights to obtain information from the data controller as to the purpose, scope and means of processing their data, and may demand that the data is corrected, updated, rectified, or even temporarily or permanently suspended if it is not complete or is outdated, untrue or collected in violation of the Data Act, or the purpose for which the data was collected no longer exists;

— data subjects may always object to the processing of their personal data for marketing purposes.

Where the privacy of a data subject has been violated due to a breach of the Data Act, he/she may also rely on the regulations contained in the Civil Code to protect his/her privacy.

Romania

John Fitzpatrick, john.fitzpatrick@cms-cmck.com
Valentina Parvu, valentina.parvu@cms-cmck.com
Gabriel Sidere, gabriel.sidere@cms-cmck.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

The primary law setting forth the legal framework regulating the electronic archiving is represented by Law No. 135/2007.

According to Law No. 135/2007 and its Methodological Norms approved by Order No. 493/2009, any natural or legal person has the right to store its documents in electronic format within an electronic archive. The management of the electronic archive system and of the stored documents is ensured via an administrator who must file a notification with the Ministry of Communications and Informational Society 30 days prior to the commencement of the archiving services (the notification must be accompanied by certain documents, including documents evidencing the security and storage measures that will be adopted). As regards registering a document within an electronic archive, Law No. 135/2007 specifies certain conditions that must be satisfied for the document to be properly registered which includes: the document bearing a valid electronic signature of the document holder, and the filing of the electronic data sheet created for the respective document and containing information interesting the document. The electronic archive must fulfil certain functional requirements including the fact that: control and security measures are in place for the documents and databases, the documents' research function exists, and access to data is ensured.

Special legislation exists with regard to electronic archiving of accounting and fiscal documents, in particular:

(i) Accounting Law No. 82/1991;

(ii) Order No. 3512/2008 regarding the accounting and fiscal documents;

(iii) Law No. 571/2003 regarding the Fiscal Code;

(iv) Government Decision No. 44/2004 for the approval of the Methodological Norms to the Fiscal Code;

(v) Order No. 488/2009 regarding the verification and homologation procedure for information systems used for issuing electronic invoices;

(vi) Order No. 870/2005 regarding the fiscal evidence register; and

(vii) Order No. 1372/2008 on the obligation to keep evidence for VAT purposes.

The Methodological Norms to the Fiscal Code approved by Government Decision No. 44/2004 provide that invoices may be stored by any means (i.e. including electronic means) and in any place, provided that the following conditions are met:

(1) the place of storage is located in Romania, except for the electronic invoices which may be stored in any place if during the storage period: the online data access is ensured, the documents' integrity is guaranteed, and the data evidencing the source authenticity and the content integrity are preserved; and

(2) in case of electronically stored documents, such documents are readily accessible by the fiscal authorities upon the authorities' request.

Issuers of electronic invoices have the obligation to use an information system which is homologated by the Ministry of Communications and Informational Society. Note that one can also outsource the electronic archiving function to third persons pursuant to the law. Further requirements set forth by the above mentioned special legislation are provided in the sections below.

With regard to personal data, the Romanian data protection law No. 677/2001 provides that personal data must only be stored for as long as the purpose of processing such personal data exists. Thereafter, data must be destroyed or archived, if such personal data are subject to the archiving legislation.

Note: The EC Data Retention Directive was implemented into Romanian legislation by Law No. 298/2008. However, such law has been recently declared as breaching the Romanian Constitution by the Decision No. 1258/2009 of the Romanian Constitutional Court. The provisions of Law No. 298/2008 were deemed to be of nature to damage the fundamental rights and freedoms of the person concerning his/her privacy, correspondence and freedom of expression.

Is there a legal definition of electronic archiving?

As indicated, the archiving of electronic documents is subject to the requirements of Law No. 135/2007 on electronic archiving, which regulates the creation, maintenance, access to and use of electronic documents archived electronically.

Law No. 135/2007 does not expressly define electronic archiving. However, pursuant to Article 4, one is permitted to "store documents in electronic format in an electronic archive for preserving purposes". Pursuant to Article 3, the "electronic archive" is defined as the "electronic archiving system together with all the archived electronic documents" and the "electronic archiving system" is "the information system designed to ensure the collecting, storage and the organisation of the documents for the purpose of preserving, accessing and reproducing them".

Under Romanian data protection law No. 677/2001, the definition of "processing" also includes data storage. Processing personal data means "any operation or series of operations that are performed on personal data, by automatic or non-automatic means, such as collecting, registering, organising, storing, adapting or altering, retrieving, consulting, using, disclosing to a third party by transmission, dissemination or by any other way, combination or alignment, blocking, erasure or destruction". Personal data is defined as "any information referring to an identified or identifiable natural person".

For accounting purposes, which records must be kept by corporations and for how long?

Under Accounting Law No. 82/1991 and Order No. 3512/2008 regarding the accounting and fiscal documents, corporations are required to keep various accounting and financial documents including accounting registers, financial statements and balance sheets.

Mandatory accounting registers include: the General Journal (where economic/financial operations are chronologically recorded), the Inventory Journal (where inventoried assets and liabilities are recorded), and the Accounts Ledger (where the movement of assets and liabilities are recorded).

Accounting registers and justificatory documents must be kept for a period of ten years from the end of the relevant financial year, except for salary registers which must be kept for 50 years. In addition, certain categories of financial and accounting documents (identified in Annex 4 to Order No. 3512/2008) may be kept for a shorter term of five years provided that the business needs of the corporation do not dictate the need for a longer term.

With the exception of the Inventory Journal, the above accounting and financial documents may be kept digitally provided certain minimum conditions, as established by Order No. 3512/2008, are satisfied (these include security measures to protect the confidentiality and integrity of the information and measures relating to the IT system used to archive data).

For tax purposes, which records must be kept by corporations and for how long?

In addition to the records which must be maintained for accounting purposes in general, fiscal legislation (in particular, the Fiscal Code, Order No. 870/2005 regarding the fiscal evidence register, and Order No. 1372/2008 on

the obligation to keep evidence for VAT purposes) requires that the following registers must be kept by a company specifically for tax purposes: a register of fiscal evidence to be kept for ten years from the date of last entry in which information used to calculate the tax base for profit tax is recorded; and a register of sales and a register of acquisitions for VAT purposes to be kept for ten years from the date of last entry.

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Specific VAT rules for electronic storage of invoices are primarily provided by Order No. 1372/2008 on the obligation to keep evidence for VAT purposes and Article 156 of the Fiscal Code. Such legislation implements into the Romanian law the provisions of Directive 2001/115/EC.

Pursuant to Order No. 1372/2008, the relevant documents may be stored by any means (i.e. including electronic means) and in any place, provided that the following conditions are met:

(1) the place of storage is located in Romania, except for the electronic documents which may be stored in any place if during the storage period the data online access is ensured and the documents' integrity is guaranteed; and

(2) in case of electronically stored documents, such documents are readily accessible by the fiscal authorities upon the authorities' request.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Electronic copies of invoices and contracts do not have the same evidential value as paper documents. Before a court of law, electronic documents only have evidential value if they are corroborated by other evidence.

Pursuant to the Electronic Signature Law No. 455/2001, an electronic document that has an "advanced" electronic signature incorporated in, attached to or logically associated with it can be assimilated from the point of view of its conditions and effects with a hand-written document. Also, an electronic document which has an electronic signature incorporated, attached to or logically associated which is acknowledged by the other party to the document has the same value as a notarised document.

The "advanced" electronic signature is based on a qualifying certificate and is created using a secured signature creation device. The qualifying certificate confirms the connection between the electronic signature and its author and is issued by a provider of certifying services, organised and functioning pursuant to the law.

How long must documents be stored to cover the most important statutory limitation periods?

The general statutory limitation periods in Romania are of three years for debts recovery - related claims (Decree No. 167/1958), and of 30 years when referring to real estate – related claims (Civil Code).

Special statutory limitation periods apply to: personal / moral rights claims, certain debts recovery – related claims, and certain real estate – related claims.

In principle, the immovable in-kind restitution claim is not subject to a statutory limitation period.

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Non-personal information Financial and accounting documents should be archived at the company's fiscal domicile or secondary headquarters. However, these documents may also be stored at third parties providing archiving service and which are based in Romania (Paragraph 50 of Annex No. 1 to Order No. 3512/2008). The Romanian fiscal authority may prohibit the storage of these documents at the company's fiscal domicile or secondary headquarters where, during an audit, the fiscal authority finds irregularities relating to the method of document archiving, and may specify a different storage location for such documents.

Personal information Any processing of personal information (including the storage of such information) must be carried out in accordance with the legal requirements of Romanian data protection law, including obtaining the data subject's prior consent to the processing of his/her personal data, observing the data subject's rights, and the notification of the processing operations by the data controller filed with the data protection regulator (Data Protection Law No. 677/2001). The transfer of personal data to non - EU Member States requires notification to and authorisation by the Romanian data protection Regulator. Authorisation of such a data transfer is conditional, in principle, upon proof that the recipient country ensures an adequate level of protection for the personal data being transferred.

Tax Electronic records may be kept in any EU Member State if both online access and the integrity of the data's content are guaranteed (Order No. 1372/2008 on the obligation to retain evidence for VAT purposes).

Must special measures be taken to ensure data security?

Non-personal information Order No. 489/2009 on the methodological norms for the authorisation of "data centres" sets out the requirements for a secured system. A "data centre" is a secured space equipped with IT and communication tools allowing the receipt, storage and transmission of data in electronic format.

The data centre needs to be authorised by the Ministry of Communications and Informational Society. For this purpose, the data centre must ensure the security and integrity of data, the availability of the electronic archiving system, and the back-up of the stored data.

Special requirements regarding the electronic signature apply (see discussion above on Law No. 455/2001 regarding the electronic signature).

Personal information Romanian data protection law No. 677/2001 sets out security requirements for the electronic storage of personal data. Data controllers are obliged to adopt adequate organisational and technical measures in order to protect personal data against unlawful or accidental destruction, loss, alteration, disclosure or non-authorised access. Such measures are detailed in Order No. 52/2002 issued by the data protection regulator.

Special security measures are imposed by Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector.

Must special measures be taken to protect the data subjects' privacy?

Personal data processing must be made by observing certain general rules, in particular:

— personal data must be processed fairly and lawfully;

— data must be collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes;

— data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

— data must be accurate and, where necessary, kept up to date; and

— data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (where the law requires that personal data must be retained for a certain period of time (e.g. employee salary registers), the retention period for such data will be determined by the applicable legislation).

Processing of personal data requires in general that the data subject's prior consent is obtained and that the local data protection regulator is notified about the processing. With regard to sensitive personal data (i.e. personal data relating, for example, to an individual's state of health or ethnic origin), the data protection regulator will conduct a prior check of the data controller following the notification of the processing and will authorize the processing (Decision No. 11/2009 on the categories of personal data operations likely to present special data protection risks). Also, the transfer of data to non-EU States is subject to prior authorisation by the local data protection regulator. The regulator will authorise the transfer if the data controller can offer sufficient guarantees to the regulator that the fundamental rights of the data subjects will be protected.

Russia

Ekaterina Lopatnikova, ekaterina.lopatnikova@cmslegal.ru;
Irina Kaletinkina, irina.kaletinkina@cmslegal.ru;
Maria Sazhina, maria.sazhina@cmslegal.ru;
Valentina Kolentsova, valentina.kolentsova@cmslegal.ru

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

There is no specific law in Russian legislation regulating electronic archiving. However, certain statutory acts set out specific requirements for electronic data storage in different spheres, including: the Federal Law on Archives in the Russian Federation (No. 125-FZ of 22 October 2004), the Federal Law on Joint-Stock Companies (No. 208-FZ of 26 December 1995) and the Federal Law on Information, Information Technology and the Protection of Information (No. 149-FZ of 27 July 2006).

Purchases books and sales books may be kept in electronic form (The Rules for Keeping Registers of Incoming and Outgoing Invoices, Purchases Books and Sales Books in Settlements on Value Added Tax (p. 28)). In this case, upon the expiry of the tax period concerned, but at the latest on the 20th of the month following the tax period, the purchases book and the sales book must be listed with numbered pages, bound and attached with a seal.

Is there a legal definition of electronic archiving?

There is no legal definition of "electronic archiving" in Russian legislation. However, the following laws regulate electronic archiving:

Federal Law on Archives in the Russian Federation (No. 125-FZ of 22 October 2004) This law regulates the archives of the Russian Federation regardless of their source or origin, time and manner of creation or the type of media (including electronic documents).

Federal Law on Joint-stock companies (No. 208-FZ of 26 December 1995) This law states that a company must ensure the register of shareholders is kept and stored in compliance with Russian Federation legislation from the time of the company's state registration. In accordance with the Decision of the Federal Commission on the securities market (No. 27 of 2 October 1997) on approval of the regulation for keeping the register of owners of registered securities, the register is a collection of data, recorded in hard copy format and/or entered into an electronic database, which is intended to identify registered persons and confirm their rights to the securities listed in the personal accounts of registered persons.

Federal Law on Mass media (No. 2124-1 of 27 December 1991) This law covers periodical publications created digitally and/or kept in databases.

Federal Law on Information, Information Technology and the Protection of Information (No. 149-FZ of 27 July 2006) This law regulates the storage of information (messages, data) irrespective of the form of their presentation, particularly in electronic form.

Federal Law on Combating the Legalisation of Illegal Earnings (Money Laundering) and the Financing of Terrorism (No. 115-FZ of 7 August 2001) This law enables organisations to carry out financial transactions in electronic form.

Federal Law on Personal Data (No.152-FZ of 27 July 2006). This law regulates the use of personal data processed electronically.

For accounting purposes, which records must be kept by corporations and for how long?

In accordance with Federal Law on Accounting (No. 129-FZ of 21 November 1996), primary and summary accounting documents may be stored in paper or electronic form. Where stored electronically, the organisation must make hard copies of such documents at its own expense for the other parties to a transaction and at the request of

regulatory bodies, in accordance with the legislation of the Russian Federation. As a general rule, organisations must keep primary account documents for at least five years.

For tax purposes, which records must be kept by corporations and for how long?

Where there is insufficient information in accounting registers to determine the tax base, the taxpayer has the right either to enter additional information in accounting registers, thus creating taxation registers, or to keep separate independent taxation registers (Article 313 of the Russian Tax Code).

According to Article 314 of the Russian Tax Code, analytical taxation registers are consolidated forms for the systemisation of tax record data for the reporting period.

Taxation registers must be kept in hard copy, in electronic form and/or on any machine-readable carriers. The form of taxation registers must be explained by the taxpayer and set out in the Appendix to the company's accounting policy (Article 314 of the Russian Tax Code).

In its letter of 24 July 2008 (No. 03-02-07/314), the Ministry of Finance of the Russian Federation clarified that primary documents, taxation and accounting registers may be stored in electronic form if otherwise not provided for by Russian legislation. However, such storage should be performed in conformity with the Federal Law on Electronic Digital Signatures (No. 1-FZ of 10 January 2002) by using an electronic digital signature, having the same effect as a hand-written signature in a hard copy document paper.

According to Article 4 (1) of Federal law No. 1-FZ, an electronic digital signature in an electronic document has the same effect as a hand-written signature in a hard copy document if the following conditions are satisfied:

— the signature key certificate relating to the electronic digital signature is valid as at the time of verification or the time of signing the electronic document;

— the authenticity of the electronic digital signature in the electronic document has been confirmed; and

— the electronic digital signature is used in compliance with the information specified in the "signature key certificate" (a hard copy or soft copy document containing the electronic digital signature).

Pursuant to Article 23 of the Russian Tax Code, the taxpayer is obliged to ensure, over the course of four years, the retention of bookkeeping and tax records, as well as the retention of other documents required for the calculation and payment of taxes and fees, including the documents confirming income earned, expenses incurred and paid (withheld) taxes.

In accordance with Article 283 of the Russian Tax Code, taxpayers are obliged to retain the documents that confirm the volume of incurred losses in the course of the entire period during which they reduce the tax base of the current tax period by the sums of the earlier incurred losses.

However, in practice it is difficult to distinguish the tax primary documents from the accounting primary documents. In this respect, it is recommended that the accounting and taxation primary documents are retained for at least five years (as provided for in Federal law "On accounting" No. 129-FZ).

The five-year period for keeping primary accounting documents is also provided for in the list of typical administrative documents resulting from the activities of organisations with time periods of storage (adopted by Rosarkhiv on 6 October 2000).

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

The Russian Tax Code does not provide specific rules regulating the electronic storage of incoming and outgoing invoices.

The official position of the Russian tax authorities is that taxpayers are not entitled to issue invoices in electronic form. The reasons for this are:

— The invoice must be signed by the head and chief accountant of the company or other officials authorised by a special order of the company (Article 169 (6) of the Russian Tax Code). This Article does not state that the electronic digital or facsimile signature of the head or chief accountant of the company may be used instead.

— In compliance with page 1 of the Rules for Keeping Registers of Incoming and Outgoing Invoices, Purchases Books and Sales Books in Settlements on Value Added Tax (approved by Decision of the Government of the Russian Federation No. 914 of 2 December 2000), buyers must keep a register of original invoices received from sellers in which the invoices must be stored and sellers must keep a register of the invoices issued to buyers in which their second copies must be stored. The registers of incoming and outgoing invoices must be bound together and their sheets numbered (page 6 of the Rules). The Rules, therefore, do not provide for the electronic storage of incoming and outgoing invoices (nor does the Russian Tax Code).

Notwithstanding the tax authorities' opinion, applicable Russian legislation states that the electronic storage of invoices is still possible and cannot be considered illegitimate. However, the rules for the issuing and storage of invoices will only be observed if the originals of invoices exist in paper form and they are duly registered in the registers of invoices. If the taxpayer does not have the original of the invoice in paper form, he will not be able to benefit from his right to VAT deduction (or recovery).

At present, there are plans to create a new system that would allow taxpayers to register invoices electronically in the Russian Federation (Guidelines regarding Russian Tax Politics for 2010, 2011 and 2012 (approved by the Government of the Russian Federation on 25 May 2009)).

As regards Directive 2001/115/EC of the EU, the Russian Federation is not obliged to implement its provisions into the Russian legislation as Russia is not a Member State of the EU.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Electronic copies of invoices do not have the same evidential value as paper invoices. As regards electronic copies of primary documents, they have the same evidential value as paper documents, provided that they were established in strict conformity with Federal Law No. 1-FZ of 10 January 2002 on Electronic Digital Signatures, as stated in Letter No. 02-14-13/1297 of the Ministry of Finance of 19 May 2006.

Invoices are not considered to be primary documents (Letter No. 03-03-06/1/478 of the Ministry of Finance of 21 August 2008) for the purposes of Federal law No. 129-FZ.

How long must documents be stored to cover the most important statutory limitation periods?

The Federal Law on Archives in the Russian Federation (No. 125-FZ of 22 October 2004) provides for the temporary storage of documents until they are handed over to state and municipal archives for permanent storage.

Different types of documents require different periods of temporary storage:

— Documents included under the established procedure in the Archive Fund of the Russian Federation and produced by Federal governmental bodies or other State bodies of the Russian Federation: 15 years;

— Documents included in the Archive Fund of the Russian Federation that are produced by governmental bodies or other State bodies and organisations or subjects of the Russian Federation: ten years;

— Documents included in the Archive Fund of the Russian Federation that are produced by local self-government bodies and municipal organisations: five years;

— Specific types of archival documents included in the Archive Fund of the Russian Federation:
  - for technological and design documentation, patents: 20 years;
  - for cinema and photographic documents: five years;
  - for video and sound documents: three years

In accordance with the Federal Law on Accounting (No. 129-FZ of 21 November 1996), organisations must keep their primary accounts documents, accounting ledgers and bookkeeping reporting information within the terms established in accordance with the rules set forth for state archive organisations, but for at least five years.

In accordance with the Federal Law on Combating the Legalisation (Laundering) of the Proceeds of Crime and the Financing of Terrorism (No. 115-FZ of 7 August 2001), documents containing information needed for the identification of a person shall be stored for a period of not less than five years. This period shall be counted from the day the client relationship is terminated.

In accordance with Decision of the Federal Commission on the Securities Market (No. 27 of 2 October 1997) on Approval of the Regulation for Keeping the Register of Owners of Registered Securities Documents, which constitutes the basis for entering records in the register, records must be stored for no less than three years from date of receipt.

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Non-personal information The Federal Law on Joint-stock Companies (No. 208-FZ of 26 December 1995) provides that a company must retain the documents specified in Clause 89.1, including accounting documents, financial statements and documents that constitute the basis for entering records in the register, which may be compiled electronically, at the location of its executive body in compliance with the procedure and for a term established by the Federal executive body in charge of the securities market.

Personal information The main regulations for processing personal data are set out in the Federal Law on Personal Data (27 July 2006, No. 152-FZ) (the "Personal Data Protection Act").

Under the Personal Data Protection Act, there are no restrictions on data centres that process personal data being located outside the premises of the company, in the same country or abroad, provided that the personal data are processed in accordance with data protection legislation. The Personal Data Protection Act sets out general requirements for processing data for any third party within Russia or abroad. A company may entrust a third party with the processing of personal data, provided an agreement is entered into by the parties. The essential condition of the agreement is the third party's obligation to ensure the confidentiality and security of the personal data being processed. Therefore, third party data processors must independently satisfy the legal requirements for processing personal data.

The main requirement for cross-border transfers of personal data and for storing data abroad is for the destination country to provide an "adequate level" of protection concerning the rights of personal data subjects. According to the Russian Personal Data Protection Authority, EU countries of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data provide an adequate level of personal data protection.

The Russian Personal Data Protection Act contains no particular established restrictions as to the data storage period. Personal data may be stored until fulfilment of the purpose for which it has been collected. Thereafter, the company must destroy the data within three working days, unless otherwise prescribed by law.

In addition, personal data may be processed only with the informed and explicit consent of the individual, except where otherwise permitted by law. This means that in giving his/her consent (for his/her personal data to be processed), an individual is entitled to receive information on the company or on any third party (group company or a outsourcing company) that processes his/her personal data; on the methods used by the company to process personal data; details of those who have access to the personal data or who may be granted access; the time limits for the processing of personal data; and the legal consequences that the processing of his/her personal data may entail vis-à-vis the individual. In cases stipulated by law, the processing of personal data (for example, sensitive data) is permitted only if an individual has given his/her consent in written form (hard copy).

There are no specific Russian tax rules regulating the storage of electronic copies of invoices by persons other than the buyers and sellers involved in the transaction (for example, data centres).

In theory, companies may have their documentation, including invoices (in paper or electronic form) stored by special organisations under storage contracts, as tax legislation does not contain any provisions prohibiting taxpayers to do this.

However, taxpayers should always be in a position to present the appropriate documents to the tax authorities upon request within a period of five days (Article 93 of the Russian Tax Code).

Must special measures be taken to ensure data security?

Non-personal information The Federal Law on Information, Information Technology and the Protection of Information (No. 149-FZ of 27 July 2006) regulates the Protection of Information. The Protection of information requires the undertaking of legal, organisational and technical measures to:

— ensure the protection of information against any illegal access, destruction, modification, blocking, copying, supply, dissemination and against other illegal actions in respect of that information;

— maintain the confidentiality of the information and limit access;

— ensure the right of access to information.

The holder of information and the operator of the information system must, in instances specified under the legislation of the Russian Federation, take measures to:

— prevent unauthorised access to information and/or transfer of information to persons having no right of access to information;

— promptly detect cases of unauthorised access to information;

— exclude the possibility of unfavourable consequences associated with the violation of the procedure for access to information;

— prevent technical information processing facilities from being affected in a way that may result in the non-functioning of the same;

— provide for the immediate restoration of information that has been modified or destroyed as a result of unauthorised access;

— ensure monitoring of the level of protection of information.

This Federal Law also regulates responsibility in the sphere of information, informational technologies and the protection of information.

Personal information Under the Russian Personal Data Protection Act, any company processing personal data must take the organisational and technical steps required by the Act. This includes using encryption (cryptographic) facilities, protecting personal data against any illegal or

accidental access, the destruction, alteration, blocking, copying, dissemination of personal data, and against other illegal actions. The IT systems dealing with personal data must be brought in line with the requirements of the Personal Data Protection Act by 1 January 2010. The methods of protecting personal data are set forth in the regulations issued by the Russian Federal Service for Technical and Export Control and by the Russian Federal Security Service of Russia. These regulations are highly technical and relate to the specification of the IT systems used for the processing of personal data.

Must special measures be taken to protect the data subjects' privacy?

Under the Russian Personal Data Protection Act, confidentiality of personal data is a requirement which is binding upon the company that has obtained access to the personal data, in order to prevent the dissemination of such data without the consent of the personal data subject or in the absence of other legal grounds. In order to protect the data subject's privacy, when processing personal data, the data processor should ensure the following:

— the prevention of unauthorised access to the personal data and/or its transfer to persons not authorised to access it;

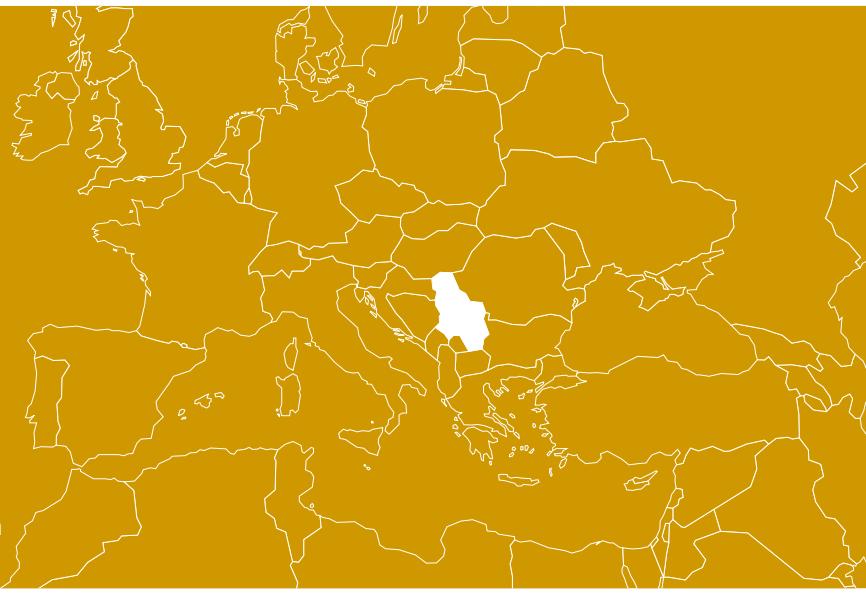
— the timely detection of any unauthorised access to the personal data;

— the prevention of the hardware being affected by automated personal-data processing tools that may disrupt its operation;

— the immediate restoration of personal data that has been modified or destroyed as a result of unauthorised access;

— the permanent monitoring of the adequate protection of personal data.

Serbia



Milica Popovic, milica.popovic@cms-rrhs.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

The legal framework governing electronic archiving in the Republic of Serbia is rather complex. As Serbia is not an EU Member State, the Data Retention Directive has not been implemented into Serbian legislation in a comprehensive manner. Instead, there are certain provisions in various pieces of legislation that resemble the Data Retention Directive provisions. Listed below is a brief summary of the key legal provisions:

The Data Protection Law (DPL) (Official Gazette of the Republic of Serbia, No. 97/08) The DPA applies to all companies and persons that have control of personal data (information from which an individual can be identified). The DPL includes data gathered electronically.

The Telecommunications Law (Official Gazette of the Republic of Serbia, No. 44/03) This sets out obligations for public telecommunications operators to retain various data, including data about users, and to submit this data to the Regulatory Agency for Telecommunications (RATEL) when required to do so. Unfortunately, the Law does not specify for how long operators are required to retain such data. The enactment of the bylaw specifying such retention periods is still pending.

The Anti-Money Laundering and Prevention of Terrorism Financing Law (Official Gazette of the Republic of Serbia, No. 20/09) This applies to a number of organisations including banks, exchange offices, investment funds, financial leasing companies, brokers and dealers, organisers of chance games, auditing companies and postal providers. The law is silent as to whether it is applicable to telecommunications providers as well. The Law sets a ten year period for the storage of information that could be needed for preventing money laundering and the financing of terrorism.

Corporation Tax The duty to maintain records for Corporation Tax purposes may generally be satisfied by the retention of the information contained in the records (including in electronic form).

VAT The VAT payer is obliged to maintain records for VAT purposes as provided for in the VAT Law (Official Gazette of the Republic of Serbia, No. 25/01) and its bylaws, for ten years following the calendar year to which the records relate. The Law on Electronic Signatures (Official Gazette of the Republic of Serbia, No. 135/04) approves record keeping in a computerized form, subject to certain conditions.

Is there a legal definition of electronic archiving?

There is no strict definition of electronic archiving established in Serbian law.

This expression essentially refers to the storage of information in a non-manual filing system. In the DPL, the concept of electronic archiving is enshrined within the broader concept of data processing. The definition of "processing" includes keeping or storing information and therefore includes "archiving".

For accounting purposes, which records must be kept by corporations and for how long?

The Law on Accounting and Auditing (Official Gazette of the Republic of Serbia, No. 46/06) This deals with the maintenance of accounting records. Every company is required to keep accounting records, in paper form or electronically, that are true records of all changes in the company's assets, liabilities, capital, income and expenses. Electronic copies of accounting records must have an electronic signature of the person responsible for its content.

The statutory period for the retention of accounting records is five years from the last day of the business year to which the records are applicable.

For tax purposes, which records must be kept by corporations and for how long?

Corporation Tax Every company is required to keep tax records, in paper form or electronically, that are true records of all changes in the company's assets, liabilities, capital, income and expenses. Electronic copies of these records must have the electronic signature of the person responsible for the documents' content. The statutory period for the retention of records used for tax purposes is five years from the last day of the business year to which the records are applicable (The Corporate Profit Tax Law, Official Gazette of the Republic of Serbia, No. 25/01, and the Law on Accounting and Auditing).

VAT The Regulation on the Form, Content and Manner of VAT Record Keeping (Official Gazette of the Republic of Serbia, No. 107/04) This provides for a detailed list of VAT records to be retained, including:

— copies of all issued and received VAT invoices;

— the amount of turnover that is VAT free;

— the amount of turnover that is subject to the general VAT rate of 18% and the VAT calculated on that amount;

— the amount of turnover that is subject to the special VAT rate and the VAT calculated on that amount;

— the amount of turnover that is subject to VAT deductions and withholdings;

— the amount of turnover abroad if it was subject to withholding tax if performed in Serbia;

— the amount of turnover that is subject to VAT deductions without withholdings;

— the amount of turnover abroad if it was not subject to withholding tax if performed in Serbia;

— the value of goods entered in the free zone, except goods for end-use in the zone;

— the value of goods entered in the free zone as end-use goods;

— the value of transport and other services provided to users of free zones which are directly related to the entering of goods in the free zone;

— the value of goods dispatched to duty free shops and the value of goods dispatched from these shops;

— the amount of turnover with Republic of Montenegro and Kosovo;

— the wholesale value of goods and services provided by companies who are not VAT payers;

— the wholesale value of goods and services with the VAT calculated;

— the amount of VAT calculated on invoices and other documents for purchased goods and services;

— the wholesale value of goods and services that are VAT free;

— the amount of advanced payments and calculated VAT;

— the amount of advanced payments;

— the value of imported goods that are subject to VAT;

— the purchase price of imported goods that are VAT free;

— issued receipts and the amount of VAT paid to agricultural producers;

— the value of goods and services purchased from the agriculture producer;

— the amount of VAT to be paid.

The tax authority requires additional records to be kept for particular trades, business activities or special schemes.

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Note that Serbia is not an EU member, and therefore, the requirements of EU law are not always transposed to Serbian legislation.

The VAT Law provides the framework, and the Law on Cash Registers (Official Gazette of the Republic of Serbia, No. 135/04) sets out the detailed procedure for the electronic storage of VAT invoices. Two copies of the invoice are issued, one for the buyer of goods/services, the other for the VAT payer. The VAT payer's copy stays in the electronic system connected to the centralized Tax Administration database. The VAT payer must send daily reports to the Tax Administration through that system. Copies of issued invoices must be kept for three years, regardless of whether they are in hard copy or electronic format.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Electronic copies of invoices and contracts have the same evidential value as paper documents.

The Law on Electronic Signatures has had the effect that paper and electronic documents have the same evidential value in all proceedings, judicial and administrative. However, there are a few exceptions for which hard copy documents are required in order to be legally binding (e.g. the transfer of real estate, gifts and estates).

How long must documents be stored to cover the most important statutory limitation periods?

The answer to this question depends on the type of documents to be archived. There is no law governing how long general contracts should be retained. However, it is important that they are kept for the duration of the relevant limitation period for bringing legal action. For claims arising from contracts, the limitation period is ten years.

More specific legal provisions apply to the storage of specialist documents, including tax documents, employment documents and corporate documents. VAT Law requires that records are kept for ten years following the calendar year to which the records relate. Copies of VAT invoices must be stored for three years from the date of issue.

The Law on Accounting and Auditing requires for financial and auditing records to be kept for 20 years. The accounting records are maintained for five years. The company book and the so-called "diary" are kept for ten years. Salaries records are maintained permanently. Auditing companies are obliged to maintain the documentation used as basis for auditing reports five years after the auditing report is submitted.

The Companies Law (Official Gazette of the Republic of Serbia, No. 125/04) This requires the Articles of association and shareholders agreement to be stored permanently, whilst the following documentation must be stored for five years:

— registration decision;

— documents approved by the shareholders' assembly and management board;

— decisions made by the company;

— decision about establishment of rep offices and branch offices;

— documents evidencing property of the company;

— minutes from shareholders' assembly and board meetings;

— financial reports, business reports and auditing reports and documents evidencing that these were submitted to the relevant authorities;

— accounting documentation and all invoices;

— book of shares;

— list of related companies;

— list of authorised representatives and members of the board;

— list of all agreements signed between the company and the manager or members of the board.

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Non-personal information There is no general legal requirement for non-personal information to be archived on company premises or elsewhere.

Personal information Any transfer of personal data outside the Republic of Serbia must comply with the DPL. Personal data may not be transferred outside Serbia unless that country or territory is a signatory of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, or unless that country ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data, equal to that provided in the Convention (subject to approval by the ombudsman for data protection).

Tax There is no requirement for electronic copies of documents to be stored within Serbia for Corporation Tax purposes.

For VAT purposes, electronic invoices are kept in the VAT payer's system and therefore must be kept in Serbia as the VAT payer's system must be connected to the centralized VAT system within the Tax Administration.

The Law on Games of Chance (Official Gazette of the Republic of Serbia, No. 84/04) This requires gambling companies to have their computer system connected to the centralized network within the Administration for Games of Chance. The Law is silent as to where gambling company servers should be kept, but the Administration requires gambling companies' servers and all electronic records required by law to be kept within the territory of Serbia.

Must special measures be taken to ensure data security?

Non-personal information In relation to confidential information that is not personal information, the person who owes the duty of confidentiality must exercise the reasonable care of a prudent man to protect the information from disclosure.

Personal information The DPL applies to "personal data"(information from which an individual can be identified).

The law requires that the data controller takes appropriate security measures to protect personal data, taking into account the cost and available technology. The ombudsman for data protection may take legal action against companies that fail to observe security measures in processing personal data, which may result in significant fines being imposed on the offender.

Must special measures be taken to protect the data subjects' privacy?

The DPL does not specify the period for which the data should be stored. The processing of personal data should be carried out in a manner that is adequate, taking into account the purpose for which the data is processed. The identity of a person must be, and must remain

anonymous. Data must not be processed in an excessive manner; it should be only be processed to the extent necessary to achieve the purpose for which it is processed.

The DPL imposes stricter rules for the processing of "sensitive personal data" (including information relating to an individual's racial or ethnic origin, criminal records, religious beliefs, sexual life, health, receipt of social aid and membership of labour unions or political parties). When processing sensitive personal data, the data controller must obtain the written consent of the data subject. Such consent to the processing of sensitive data may be withdrawn at any time.

Slovakia

Ian Parker, ian.parker@cms-cmck.com
Hana Supekova, hana.supekova@rc-cms.sk

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

The principal requirements for electronic archiving are regulated by the following acts:

Act No. 428/2002 Coll. on Personal Data Protection as amended (Act on Personal Data Protection) This Act applies to all natural or legal persons who process personal data, determine the purpose and means of processing or provide personal data for processing. The Act states that personal data may only be processed in compliance with the personal data processing principles which apply to archiving as one form of personal data processing.

Act No. 610/2003 Coll. on Electronic Communications as amended (Act on Electronic Communications) Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive) has been implemented into the Act No. 610/2003 Coll. on Electronic Communications as amended (Act on Electronic Communications). The Act states that providers of publicly available electronic communications services or public communication networks must retain data they have generated or processed providing the service or network, for the purpose of the investigation, detection and prosecution of serious crime. The provider should store traffic and location data, data relating to the communicating parties and information relating to and necessary for identifying the subscriber or registered user, for six months, where related to internet access, internet electronic mail and internet telephone calls. The data relating to other types of communication must be stored for 12 months. The obligation to store data includes unsuccessful call attempts but does not include unconnected calls. It is prohibited to retain data relating to the content of the communication, unless such storage is a substantial part of the service provided. There is a finite list of data that must be retained. All data and information can only be retained in electronic form.

Act No. 215/2002 Coll. on Electronic Signature as amended (Act on Electronic Signature) This defines the storage of electronic documents signed by a guaranteed electronic signature. Certain conditions determined by the National Security Authority must be met by an accredited certified authority when storing electronic documents signed by a guaranteed electronic signature.

Act No. 431/2002 Coll. on Accounting as amended (Act on Accounting) This sets out the specific requirements of electronic archiving for accounting purposes. An accounting entity may convert accounting records from one format into another as all forms of accounting records are equivalent, whether hard copy or soft copy. Where the accounting entity keeps records in an electronic form, it must have at its disposal such equipment, carriers and devices that enable such records to be converted into an easily readable form and to provide the documents in hard copy and electronic form when requested by authorised persons. The accounting entity is subject to this obligation for as long as and to the extent that it is required to maintain and archive accounting records.

Act No. 222/2004 Coll. on Value Added Tax as amended (Act on VAT) This is concerned with the requirements of electronic archiving for tax purposes and states that invoices issued by electronic means must be legible and may not be modified over the course of a filing period.

Is there a legal definition of electronic archiving?

There is no strict legal definition of electronic archiving established in Slovak law.

Electronic archiving is regulated by the Act on Electronic Communications, where providers of publicly available electronic communications services and public communication networks must retain electronically certain data generated or processed by the provision of their service or network.

The following data security principles, in addition to the technical and organisational measures for the protection of networks and services, must be kept by providers when archiving data:

— the stored data must be of the same quality and subject to the same security and protection as those data on the network;

— the data must be subject to appropriate technical and organisational measures to protect it against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

— the data must be subject to appropriate technical and organisational measures to ensure that it can only be accessed by specially authorised personnel;

— the data, except the data that has been accessed and retained, must be destroyed at the end of the retention period (Article 59a Section 6, 8, 11 of the Act on Electronic Communications).

The Act on Electronic Signatures defines the storage of electronic documents signed using a guaranteed electronic signature as an accredited certified service. Storage can only be provided by an accredited certified authority. Decree No. 132/2009 Coll. on Conditions for the Provision of Accredited Certified Services and on Requirements on Auditing, Auditing Extent and Qualification of Auditors (Decree on Provision of Accredited Certified Services) issued by the National Security Authority, stipulates the requirements for the long-term archiving of electronic documents signed by a guaranteed electronic signature. The following requirements must be observed by the accredited certified authority:

— the electronic document must be displayed in such a way that enables detection of its content;

— the document's integrity must be maintained- confirmation that the document was not changed and is accessible in the state in which it was saved in the archive;

— the document's authenticity must be maintained- confirmation, that the document was created and signed by the person who signed the document;

— evidence and storage of information important in terms of the document's existence, data on takeover, the document's storage form, the document's access and the type of storage media;

— the exercise of such activities related to the ability to edit the electronic document, which enable maintenance of the incontestability of the document's existence and data integrity and to ensure their required accessibility.

(Article 3 Section 5 of the Decree on Provision of Accredited Certified Services).

The concept of electronic archiving is also regulated in the Act on Personal Data Protection, which defines the storage of personal data as a form of data processing. (Article 4 Section 1 Letter a) of the Act on Personal Data Protection).

For accounting purposes, which records must be kept by corporations and for how long?

The maintenance of certain accounting documentation is required by the Act on Accounting. This provides that an accounting entity must keep the following accounting documentation:

a) financial statements and annual reports must be archived for ten years following the year to which they relate;

b) accounting documents, books of accounts, lists of books of accounts, lists of numerical codes or of other symbols and acronyms used in bookkeeping, a depreciation schedule, inventory lists, stocktaking reports and the accounting schedule must be archived for five years following the year to which they relate;

c) accounting records which contain information relating to the method of bookkeeping and which the accounting entity uses as evidence of bookkeeping must be archived for five years following the year in which they were last used;

d) other accounting records must be archived for a period of time set in the accounting entity's registry plan;

e) accounting records relating to ongoing tax, administrative, criminal, civil or other proceedings must be kept by an accounting entity until the end of the accounting period following the accounting period in which the deadline for their examination expired;

f) accounting documents and other accounting records relating to warranty periods and complaint procedures must be kept for the duration of the warranty periods or complaint procedures;

g) accounting records relating to uncollected receivables or outstanding payables must be kept until the end of the accounting period following the accounting period in which they were collected or paid;

h) books of analytical records for receivables, books of analytical records for payables, accounting documents and other accounting records arising directly from foreign relations before 1 January 1949, as well as financial statements relating to the transfer of property to other legal or natural persons, must be kept by the accounting entity until consent for their disposal is given by the Ministry of Internal Affairs.

As accounting records, the accounting entity may use payroll sheets, tax documents or other documentation provided such documentation meets the requirements for accounting records (Articles 35 and 36 of the Act on Accounting).

For tax purposes, which records must be kept by corporations and for how long?

The following records must be kept by taxpayers:

a) records of all supplied/received goods and services;

b) records of the supply of goods and services to another member state; records shall also contain information on supply of goods where the ownership right has not been changed, i.e. in cases where the taxpayer for the purposes of his business supplied goods to another Member State;

c) records of acquired goods from another member state; records shall also contain information on acquired goods from another Member State, where the ownership right has not been changed, i.e. in cases where the taxpayer for the purposes of his business transferred goods from another Member State;

d) records of received services from another Member State; the taxpayer shall keep separate records on received services from another Member State where he is subject to the duty to pay tax (self-billing);

e) records of imported goods;

f) records of received/made payments before supply of goods and services;

g) records of goods from another Member State, on which manufacturing work is performed (concerning tangible property) for an entrepreneur from another Member State with a VAT registration number;

h) records of goods acquired from another Member State by non taxable persons obliged to register for VAT due to an excess of the value of acquired goods from another Member State;

i) records of supplied returnable packages together with goods and returned packages; this applies to manufacturers introducing beverages on the domestic market, including importers of beverages from another Member State or a third country;

The above-mentioned records must be kept for ten years.

The following invoices are to be kept:

a) copies of invoices on supply of goods or services issued by the taxpayer or on his behalf by the customer or another person;

b) original invoices on received goods and services;

c) records of transfer of goods to/from another Member State.

These records must be stored by the taxpayer for a period of ten years following the year to which they relate. The duty to store invoices for ten years, from the year to which they relate, also applies to taxable persons not registered for VAT. Any entity that occasionally sells/buys a new vehicle to/from another member state (entrepreneurs not registered for VAT or non-taxable legal entities) must store the invoices for a period of ten years following the year of sale or purchase. A taxpayer is obliged to store import and export documents certified by the customs authority for a period of ten years from the end of the year to which they relate.

The provisions of the Act No. 511/1992 Coll. on Administration of Taxes and Fees and Changes to the System of Local Financial Authorities as amended (Act on Administration of Taxes) apply when storing the records and documents. The Act states that is possible to levy tax or the tax difference for ten years from the end of a calendar year in which the duty to submit a tax declaration or notification has arisen.

Act No. 595/2003 Coll. on Income Tax as amended (Act on Income Tax) refers to the Act on Accounting with regard to the storage of the obligatory evidence of records related to the payroll agenda (Article 39 Section 8 of the Act on Income Tax). The accounting entity in the registry plan specifies the storage period. Payroll agenda consists of records of evidence for the calculation and taxation of wages and evidence of execution of statutory wage deductions.

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

The rules for the electronic storage of incoming and outgoing invoices require invoices to be legible unmodified over the course of the archiving period, which is a period of ten years following the year to which they relate. Invoices issued by electronic means must be signed by an electronic signature to ensure the reliability of their origin and the undamaged state of the invoice's content. (Article 75 Section 6 and Article 76 of the Act on VAT)

The Act on VAT does not explicitly regulate the storage place of documents to be archived. However, the place of storage must include a detailed registry plan. (Article 16 of the Act No. 395/2002 Coll. on Archives and Registries and on Amendment of Certain Acts as amended).

The Directive 2001/115/EC amending the Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax (Invoicing Directive), has been implemented in the Act on VAT and as mentioned above, determines the rules for electronic invoicing and the electronic storage of invoices.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Invoices may be issued in hard copy or electronically with the consent of the customer. An electronic signature must be used to verify the reliability and unmodified content of

the original. These requirements guarantee the same evidential value of invoices issued electronically as invoices issued as paper documents. (Article 75 Section 6 of the Act on VAT.)

A contract concluded by electronic means has the same evidential value as a hard copy contract provided it is maintained securely so as to ensure that it cannot be modified from the final version agreed with the other party, and the contract can be presented in this version at any time to the other party to the contract (Article 5 Section 2 of the Act No. 22/2004 Coll. on Electronic Commerce as amended) (Act on Electronic Commerce).

Contracts whose effectiveness is determined by the court, a public authority or a notary's decision and contracts securing obligations cannot be concluded electronically (Article 5 Section 8 of the Act on Electronic Commerce).

Where an original hard copy contract or invoice is converted into electronic form, the electronic form does not have the same evidential value as the hard copy. Likewise, where an original electronic contract or invoice is converted into a hard copy form, the hard copy does not have the same evidential value as the electronic form.

How long must documents be stored to cover the most important statutory limitation periods?

It is important to keep all documents for as long as the relevant limitation period for bringing legal action applies. In civil matters, the general statutory limitation period is three years (Article 101 of the Act No. 40/1964 Coll. Civil Code as amended) (Civil Code) and in commercial matters, four years. (Article 397 of the Act. No. 513/1991 Coll. Commercial Code as amended) (Commercial Code).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Non-personal information There is no requirement to store electronic copies of documents containing non-personal information at the company's premises. Documents containing this information can be stored in an EU country or in a non-EU country. Slovak law does not specify where documents should be stored.

Personal information Electronic copies of documents containing personal data can be stored in any EU country or in a non- EU country. Storing personal data outside of the EU requires certain requirements to be satisfied. The transfer of personal data outside of the EU requires the approval of the Personal Data Protection Office.

Tax From a tax perspective, there is no legal restriction on the storage of electronic copies of documents outside of the company's premises, either in an EU country or non-EU country.

VAT Similarly for VAT purposes, there is no restriction on storing copies of invoices outside of the company's premises, in an EU country or non- EU country. With regard to the implementation of the Invoicing Directive into the Act on VAT, this does not contain special provisions on where copy invoices must be stored.

Must special measures be taken to ensure data security?

Non-personal information The provisions dealing with the security of non-personal information state that for accounting purposes, such documentation must be protected against loss, destruction or damage by the accounting entity.

For tax purposes, measures must be taken to ensure the authenticity of the origin of invoices, the integrity of their content and their legibility over the filing period; electronically issued invoices must be legible and may not

be modified. When archiving an entity's documents using a commissioned third party, a confidentiality obligation relating to the documents to be archived is usually set out in the storage agreement.

Personal information Special measures should be taken to ensure personal data security, pursuant to the Act on Personal Data Protection. Personal data are data from which a living individual can be identified. The controller is responsible for the security of personal data by protecting it against loss, alteration, damage, unauthorised access and also against any unauthorised forms of processing. For this purpose, the data controller must take appropriate technical, organisational and personal measures with regard to the available technology, the risk of security violation of the filing system and the importance of the processed personal data.

Must special measures be taken to protect the data subjects' privacy?

The Act on Personal Data Protection contains principles on the protection of the data subject's privacy at a national level (the principles specified in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data have been implemented by this Act).

Personal data may be processed subject to obtaining the consent of the person whose data are processed (the data subject). This consent shall be given in certain cases specified by the Act on Personal Data Protection in writing. Such consent can be withdrawn by the data subject at any time.

Data must only be obtained in accordance with the law and for a specific purpose. Only personal data that is necessary to fulfil the purpose of the processing determined by law or the processor should be processed.

The storage period of personal data depends on the purpose for which personal data are processed. After fulfilment of this purpose, personal data must be destroyed without delay.

Only accurate, complete and updated personal data can be storage for the determined purpose. Inaccurate or incomplete personal date, which cannot be corrected, must be clearly marked and destroyed as soon as possible by the data controller.

The data controller must take appropriate steps to protect personal data from unlawful damage, alteration, loss, unauthorised access or unlawful forms of processing.

Where personal data is processed in an EU country, measures must be taken to ensure it is processed in accordance with law of the respective EU country.

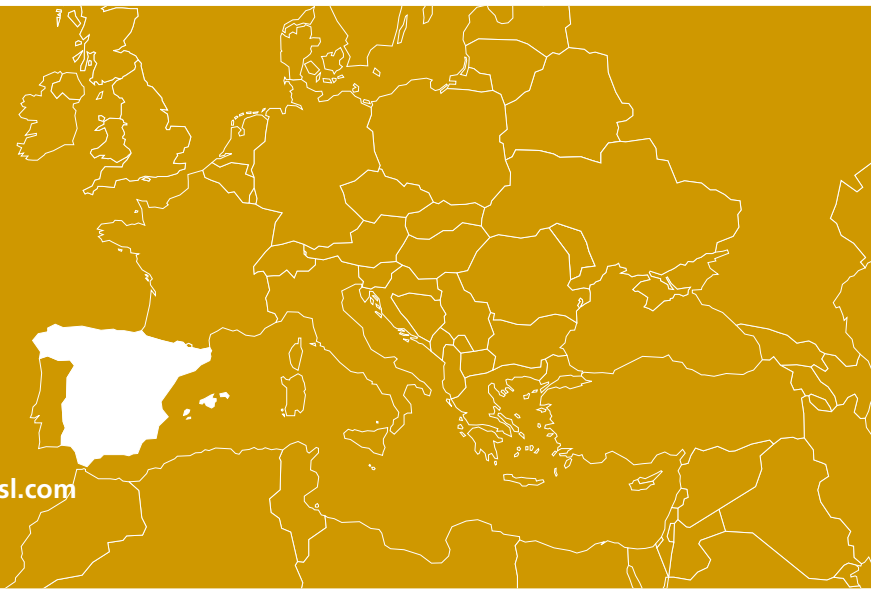
The storage of sensitive personal data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of political parties or movements, trade-union membership, biometrical data or data concerning an individual's health or sex life, is prohibited, unless explicit written consent is given by the data subject.

Data concerning breach of criminal or civil law, provisions of the misdemeanours act or execution of effective judgements or decisions, may only be processed by persons authorised to do so by law.

The data controller and processor are obliged to maintain the confidentiality of personal data within the processing period and also following termination of the processing period.

The relevant provisions of the Civil Code and the Constitution of the Slovak Republic in connection with the protection of privacy must be complied with where personal data is stored or processed.

Spain



José Manuel Rodríguez, jmrodriguez@cms-asl.com
Ana Jimenez, anjimenez@cms-asl.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

The EC Data Retention Directive 2006/24/EC The EC Data Retention Directive 2006/24/EC was implemented into Spanish law under Law 25/2007 of 18 October on the retention of data relating to electronic communications and public communications networks. This requires telecoms operators to retain certain data relating to electronic communications and make this data available to the following authorised agents: members of the police force authorised in relation to criminal investigations; National Intelligence Centre staff; and senior Customs officials. This data must be retained for 12 months from the date of the communication. This period may be reduced to six months or extended to two years, in accordance with regulatory developments.

Article 106 of the Security Measures Regulation (RD 1720/2007) The archiving of documents or media must follow the criteria set out in Article 106. These criteria are aimed at ensuring the proper preservation of documents, locating and consulting information and enabling the exercise of certain rights by the data subject including the right to object to data being processed and the right to access, rectify or cancel this data. Where there is no criteria applicable to a particular document, the data controller must establish its own criteria and procedures to be followed.

There are no specific tax regulations as regards archiving for tax purposes, aside from the specific regulations relating to electronic invoices.

Is there a legal definition of electronic archiving?

There is no strict legal definition of electronic archiving in Spanish law.

Article 107 of the Royal Decree 1720/2007 of 21 December on Storage Devices (for example, CDRW, DVDRW, USB and hard disk), sets out requirements for electronic archiving and provides that storage systems for documents containing personal data must incorporate a mechanism restricting access to these documents. Where such a mechanism cannot be incorporated, the data controller must adopt other measures to prevent unauthorised access to personal data.

The electronic archiving of personal data is defined as a type of data processing (operations and technical processes, whether or not by automatic means, which allow the collection, recording, storage, adaptation, modification, blocking and cancellation, as well as the transfer of data, resulting from communications, consultations, interconnections and transfers).

For accounting purposes, which records must be kept by corporations and for how long?

Accounting records, including receipts and all documents relating to company business, must be kept for a six-year period (Article 30 of the Commercial Code). The same requirements apply to all types of companies. The accounting records must show the company's activity.

For tax purposes, which records must be kept by corporations and for how long?

Accounts, receipts and all documents relating to company business must be kept for six years from the date of the last entry (Article 30 of the Commercial Code).

Invoices must be kept for four years from the last date of the legal period available to declare such an invoice in the VAT returns, as prescribed by statute (Article 19 Royal Decree 1496/2003 of 28 December on invoicing obligations).

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Where electronic invoices are stored outside Spain, the taxpayer must make the invoices or stored information available to the Spanish tax authorities without undue delay whenever requested. The electronic storage of invoices outside Spain is only permitted where full and immediate online access to the invoices is guaranteed. Storage of invoices in a country with which there is "mutual assistance" agreement, similar in scope to that laid down by Directives 76/308/EEC and 77/779 EEC and by Regulation (EEC) No. 218/92, will only be accepted when storage is undertaken by the taxpayer himself (following notification to the Tax Administration) or by third parties duly authorised on a case by case basis by the Tax Administration (Article 9 Order 962/2007 of 10 April (this order develops certain electronic invoicing and storage of invoice provisions contained in Royal Decree 1496/2003 of 28 November)).

Generally, taxpayers must store invoices in their original form. However, they are also entitled to elect for either the certified scanning of invoices or the storage of authenticated printed versions. A number of conditions must be met in order to use either of these alternatives (Articles 6 to 8 Order 962/2007 of 10 April).

Electronically-stored invoices must be legible and taxpayers must, at the Tax Administration's request, interpret and/or decipher data that are not self-explanatory (Article 5.3 Order 962/2007 of 10 April).

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

For litigation purposes, electronic copies of invoices are susceptible to challenge. Electronic documents, such as contracts or any other document or report, have the same evidential value as hard copies. Article 326 of the Law 1/2000 of the Civil Procedure Rules.

Electronic documents can be challenged in the same way as any other paper document. Where electronic documents are challenged, the party that has provided the electronic copy must demonstrate that the document complies with Article 3.8 of the Law 59/2003 on Electronic Signatures.

For tax purposes, electronic copies of invoices have the same evidential value as hard copy originals, provided they are certified scanned copies. (Article 17, 18 and 19 of the Royal Decree 1496/2003).

How long must documents be stored to cover the most important statutory limitation periods?

Under Spanish tax law, documents must be stored for a period of four years following the deadline for filing the relevant tax return (Articles 66 and 67 of Law 58/2003 of 17 December, General Tax Law).

The length of time for which documents should be stored depends on the type of documents to be archived. There is no law governing how long general contracts should be stored. However, it is important that they be kept for as long as the relevant limitation period for bringing legal action applies. For contracts, the limitation period is 15 years.

More specific legal provisions apply to the storage of specialist documents, employment documents and corporate documents. Companies have the obligation to store, for a period of six years, any company-related documents including: minutes of board meetings and shareholder meetings, any correspondence, account books and minute books (Article 30 of the Commercial Code).

With regard to health and safety records, the law states that medical reports must be retained for a minimum period of five years. For certain diseases, investigation, or epidemic-related reasons, these documents must be stored for longer periods (Article 17 of Law 41/2002 on regulation of the patient's autonomy and the rights and obligations regarding information and clinical documentation).

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

Non-personal information Under Spanish law, provided electronic copies are stored within the same company, there is no restriction on storing electronic copies either within or outside the particular EU member state. Data centres may be used to store electronic copies containing non-personal information.

Personal information Under Article 102 of Royal Decree 1720/2007, a back-up copy of the data and relevant data recovery procedures must be kept in a different location to the computer processing equipment. It is necessary to comply with the security requirements set out in Royal Decree 1720/2007 or incorporate measures to ensure the integrity and recovery of the data.

The back-up copy of personal data must be kept off company premises. If the back-up copy is stored in another EU country by a data processor, this will not be considered an international data transfer. However, it will be necessary for the data controller to enter into a data processing agreement with that particular data processor.

If the back-up copy is stored in a non-EU country, this will be considered a transfer of personal data outside the EEA. Therefore, the transfer will need to be authorised by the Director of the Spanish Data Protection Agency.

Tax Electronic copies of invoices need not be stored on company premises and may be stored in a different country (in any jurisdiction) provided full online access without undue delay can be guaranteed. This is in compliance with Directive 2001/115/EC which has been implemented into Spanish law.

Must special measures be taken to ensure data security?

Data controllers and (where applicable) data processors must adopt appropriate technical and organisational measures to ensure the security of personal data and prevent the alteration, loss, unauthorised processing of or access to personal data, taking into account the technology available, the nature of the data stored and the risk to which the data is subject, whether due to human action or the physical location in which the data is stored (Section 9 of the Spanish Data Protection Act 15/1999).

Regulations (Royal Decree 1720/2007 of 21 December) set out the data security measures to be complied with by those intervening in automated personal data processing and in relation to automated files, processing centres, premises, equipment, systems and programmes.

Must special measures be taken to protect the data subjects' privacy?

The Spanish Data Protection Act requires that the data controller of the corresponding data file:

— obtains and processes the data with the specific consent of the data subject (consent which, to be valid, requires that the data subject is provided with such information relating to the proposed processing of their data so as to provide an informed consent), unless any of the exceptions to this provided under the law apply (i.e. where the processing is necessary for the management of a contractual relationship between the data controller and data subject, the data subject's consent need not be obtained);

— informs the data subject of certain aspects of the data processing (which are specified by law), unless any of the exceptions provided under the law apply.
It should be noted that these exceptions are not the same as those which allow personal data processing without consent and, therefore, in certain circumstances, whilst consent is not required, the data subject must be duly informed (i.e. if the processing is necessary for the management of a contractual relationship between the data controller and the data subject, consent is unnecessary, but the data subject must be informed of the nature of the processing);

— maintains the data in such a way as to ensure its integrity;

— incorporates certain security measures provided in detail in a specific regulation, which includes the obligation to draft and have at the registered offices of the controller for inspection by the Data Protection Agency, the corresponding security measures and incidences register;

— facilitates data subjects exercising their rights of access, cancellation, rectification and objection to processing, with regard to their personal data, as provided by the Spanish Data Protection Act;

— does not communicate the data to any third parties (including companies within the same group) without the specific consent from the data subject, unless any of the exceptions specifically provided under the Act apply;

— does not transfer the data to any foreign countries, unless any of the exceptions specifically provided under the Act apply; and

— registers the personal data files at the Spanish Data Protection Registry and provides any further notifications required in a timely fashion.

Article 7 of the Spanish Data Protection Act states that personal data which refer to an individual's ethnic origin, health or sex life (sensitive personal data) may be collected, processed and shared only when, for reasons of general interest, this is provided by law or the data subject has given his explicit consent.

Ukraine

Olga Belyakova, olga.belyakova@cms-cmck.com
Andriy Buzhor, andriy.buzhor@cms-cmck.com
Svitlana Kulish, svitlana.kulish@cms-cmck.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving

The key legal provisions governing electronic archiving in the Ukraine are as follows:

Law of Ukraine "On Electronic Documents and Electronic Documents Exchange" This applies to the parties to the electronic document exchange. All electronic documents must be stored in accordance with the following requirements:

— the information contained in electronic documents must be accessible for future use;

— the electronic document must be capable of being restored to the format in which it was created, sent or received;

— information (if any) which identifies the origin and purpose of the electronic document, as well as the date on which it was sent or received, must be recorded and stored.

The parties may use data archiving companies to provide electronic document storage services, provided the above requirements are fully met.

Law of Ukraine "On Protection of Information in Information and Telecommunication Systems"
The conditions for data archiving in a system are specified by the system owner in accordance with a contract concluded between the respective system owner and the owner of data, unless otherwise provided by law.

Information owned by the state or with restricted access status (protected in accordance with the law), must be secured in a system that complies with "conformity requirements". Such requirements must be approved by state expert appraisal in accordance with the procedure provided for by law.

Is there a legal definition of electronic archiving?

There is no strict definition of electronic archiving established in law. However, the Ukrainian law "On Electronic Documents and Electronic Documents Exchange" classes "data" as information provided in a form suitable for the electronic processing.

The Ukrainian law "On Protection of Information in Information and Telecommunication Systems" defines "information processing in a system" as the performance of one or more operations, including: the obtaining, recording, transformation, reading, storage, destruction, registration, receipt and transmission of data, to be carried out in an IT system using automated means.

Electronic archiving is the storage of information provided in a format suitable for electronic processing by automated means.

For accounting purposes, which records must be kept by corporations and for how long?

Every company is obliged to keep accounting records in order to provide dedicated users with:

— the history of transactions and results of business activity

— the flow of monetary funds

— the information required for making business decisions

Accounting records must always be supported by the basic source documents (contracts, invoices, protocols of acceptance, receipts).

Tax reports (returns and declarations) must be based on the figures reflected in the accounting records.

It is recommended that accounting records be kept in electronic form, however this is not compulsory.

For tax purposes, which records must be kept by corporations and for how long?

Corporate Profit Tax There is no legislative requirement for keeping special records for corporate profit tax purposes.

A taxpayer is obliged to retain all supporting documents (basic source documents) related to its business activity. These documents are used to confirm amounts of gross income/ deductible expenses and depreciation reflected by a taxpayer in a tax declaration.

The tax declaration must be filed in the 40 days following the end of reporting period, which is a quarter.

Tax declarations and supporting documents must be preserved for at least three years from the end of relevant reporting period.

VAT Every company, being registered as VAT-payer, must keep a register/ list of incoming and outgoing VAT invoices. This register may be kept either in electronic form or as a hard copy. The following applies to VAT filing:

— VAT invoices must be kept only in hard copies.

— A taxpayer is obliged to keep all supporting documents confirming its input VAT. Ukrainian legislation does not envisage a separate VAT account.

— The VAT return must be filed in the 20 days following the end of reporting period, which is a month.

— VAT returns and supporting documents must be preserved for at least three years from the end of relevant reporting period.

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

Ukrainian legislation does not specify VAT rules for the electronic storage of incoming and outgoing invoices.

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Generally, Ukrainian legislation allows legal documents to exist in electronic form through the use of an electronic signature (except where otherwise provided by law). Such electronic documents have the same evidential value as paper versions. However, in practice, most contracts are still concluded in paper form using real signatures.

For tax purposes, electronic copies of documents (including contracts and invoices) are not admissible as evidence in any proceedings before the tax authority.

Only tax declarations and VAT returns can be filed to the tax authorities in electronic form, provided that this is agreed with tax authority and any electronic signatures used are duly registered. To date, such method of filing tax declarations is not widely used in Ukraine.

How long must documents be stored to cover the most important statutory limitation periods?

Ukrainian law states that the retention period for electronic documents may not be shorter than the retention period specified by legislation for hard copy documents.

Should such retention period prove impossible to achieve, electronic documents must be copied onto several data carriers and then periodically copied. Where this is

impracticable, electronic documents must be printed out and stored in hard copy form.

When copying an electronic document from an electronic data carrier, the integrity of the data contained on the carrier in question must be verified.

Currently, the Ukrainian central authority on archives determines limitation periods for the 2293 types of documents it has listed.

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

There is no express requirement in Ukrainian law to store electronic copies on company premises. The electronic document exchange and storage procedure will be specified by either State authorities, local self-administration bodies, companies, institutions or organisations, depending on the nature of the document.

The parties to the electronic document exchange must store the documents on electronic data carriers in a format that allows the integrity of such documents to be verified.

Must special measures be taken to ensure data security?

Personal information The conditions for processing personal information in a database are specified by the system owner in accordance with a contract entered into with the information owner, consenting to such storage, unless legislation provides otherwise. Storage of any personal data without the direct written consent of the information owner is illegal.

Non-personal information Information owned by the State or with restricted access status (protected by law), must be securely held in a system that complies with "conformity requirements". Such requirements must be approved by State expert appraisal in accordance with the procedure provided for by the law.

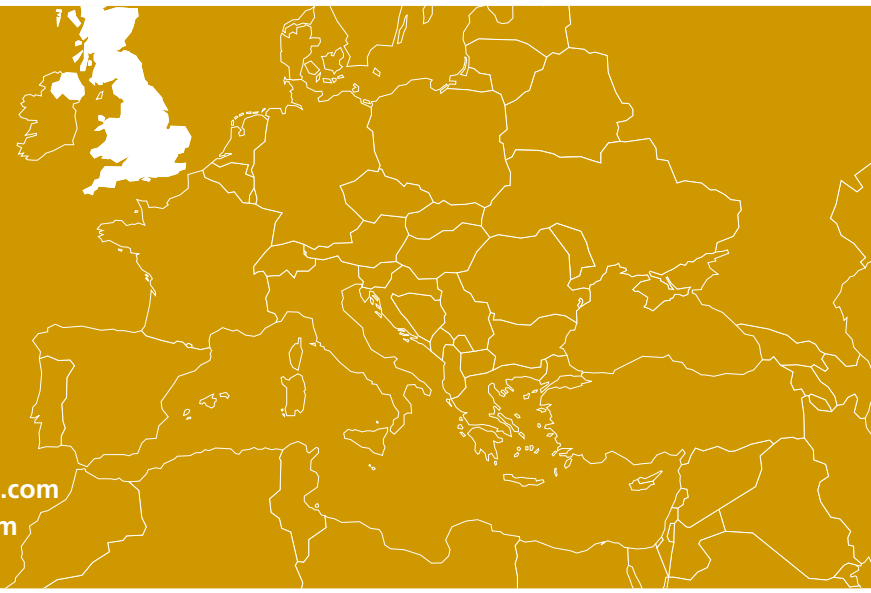
Must special measures be taken to protect the data subjects' privacy?

Ukrainian legislation sets out the general principles of protection of the data subject's privacy. In particular, the Constitution of Ukraine guarantees the privacy of mail, telephone conversations, telegraph and other correspondence and prohibits any collection, storage, use and dissemination of confidential information about a person without his or her consent with the exceptions envisaged by legislation, and only in the interests of national security, economic welfare and human rights. The Law of Ukraine "On Information" prohibits the collection of personal data without the approval of the individual involved.

Generally, there are no special procedures, obligations or separate measures that must to be taken to protect the data subject's privacy; however a person whose rights has been violated in that regard is entitled to protect their rights in court.

It must be noted, however, that the Draft Law "On personal Data Protection" provides for tighter regulation of an individual's data protection.

United Kingdom



Ian Stevens, ian.stevens@cms-cmck.com
John Armstrong, john.armstrong@cms-cmck.com
Richard Croker, richard.croker@cms-cmck.com

Please provide a brief overview of the principal requirements of the legal framework regulating electronic archiving.

The legal framework governing electronic archiving in the UK is complex. Listed below is a brief summary of the key legal provisions.

Data Protection Act (DPA) This applies to all companies and persons that have control of personal data - "data controllers". Personal data is information from which a living individual can be identified. The DPA states that such information should be held in accordance with eight data protection principles each of which are relevant to archiving personal data.

Data Retention (EC Directive) Regulations 2009 (derived from the EC Data Retention Directive) Certain information gathered from fixed and mobile telephone networks, internet, e-mail and internet telephony operated by a public communications provider should be retained for 12 months. This includes information about a call or internet use, such as the time of the call or use, its source number or IP address, the destination phone number, e-mail addresses, the geographical location of mobile phones in a call and the duration, but not the content of such communications.

Anti-Terrorism Crime and Security Act 2001 This Act applies to all postal and telecommunications providers. It allows the Home Office to impose a longer storage period for information that could be needed for preventing terrorism and safeguarding national security. A non-legally binding code of conduct published under this Act says that, generally, information that could be used for these purposes should be kept for 12 months.

Corporation tax The duty to maintain records for corporation tax purposes may generally be satisfied by the preservation of the information contained in the records (including in electronic form), with the exception of vouchers and certificates etc which show tax credits or deductions at source of UK or foreign tax (e.g. dividend vouchers, interest vouchers) and evidence of tax deducted from payments to sub-contractors under the construction industry scheme, all of which must be preserved in their original form (Paragraph 22 Schedule 18 Finance Act 1998).

VAT The duty to maintain records for VAT purposes may be discharged by presenting the information contained in the records in any form and by any means (Paragraph 6(4) Schedule 11 VAT Act 1994; Paragraph 5 Schedule 7 Finance Act 2008). Record keeping in computerised form has been approved subject to certain conditions (regulation 13A VAT Regulations 1995).

Is there a legal definition of electronic archiving?

There is no strict definition of electronic archiving established in law. This expression essentially refers to the storage of information in a non-manual filing system. In the DPA, the concept of electronic archiving is enshrined within the broader concept of data processing. The definition of data includes: “information being processed by means of equipment operating automatically in response to instructions given for that purpose”. The definition of “processing” includes holding or storing information and therefore includes “archiving”. The DPA only applies to personal data.

For accounting purposes, which records must be kept by corporations and for how long?

Sections 386 to 389 of the Companies Act 2006 deal with the maintenance of accounting records (in respect of financial years starting on or after 6 April 2008). Every company is required to keep accounting records that are sufficient:

— to show and explain the company's transactions; and

— to disclose with reasonable accuracy, at any time, the financial position of the company at that time; and

— to enable the directors to ensure that any accounts required to be prepared comply with the requirements of the Companies Act 2006 (and, where applicable, of Article 4 of the IAS Regulation).

The records to be kept should contain details of monies received and expended; details of assets and liabilities; statements of the stock held at the end of the financial year; and, except in the case of goods sold by way of ordinary retail trade, statements of all goods sold and purchased, showing the goods and the buyers and sellers in sufficient detail to enable them to be identified. These accounting records must be preserved:

— in the case of a private company, for at least three years from the date on which they are made; and

— in the case of a public company, for at least six years from the date on which they are made.

For tax purposes, which records must be kept by corporations and for how long?

Corporation Tax Records which must be kept for corporation tax purposes include all records of all receipts and expenses in the course of the company's activities and the matters in respect of which the receipts and expenses arise and, in the case of a trade involving dealing in goods, all sales and purchases made in the course of the trade. The duty to preserve records includes a duty to preserve all supporting documents (meaning accounts, books, deeds, contracts, vouchers and receipts).

The records must be preserved for six years from the end of the relevant accounting period. If the company is required to deliver a corporation tax return by notice given before the end of that six year period, the records must be preserved until any later date on which an enquiry into the return (if there is one) is completed or, if there is no enquiry, the tax authority no longer has the power to enquire into the return. If the company is required to deliver a company tax return by notice given after the end of that six year period and has in its possession at that time any records that may be needed to enable it to deliver a correct and complete return, it must preserve those records until the enquiry is complete, or, if there is no enquiry, the tax authority no longer has the power to enquire into the return. (Paragraph 21 Schedule 18 Finance Act 1998)

VAT Records which must be kept for VAT purposes include:

— business and accounting records;

— the VAT account;

— copies of all VAT invoices issued;

— all VAT invoices received;

— all certificates prepared by the company relating to acquisitions of goods from other Member States or given relating to supplies by the company of goods or services providing that those acquisitions or supplies are either zero-rated or take place outside the UK;

— documentation received relating to acquisitions of goods from other Member States;

— copy documentation issued by the company relating to the transfer, dispatch or transportation of goods by the company to other Member States;

— documentation received relating to the transfer, dispatch or transportation of goods to other Member States;

— documentation relating to importations and exportations by the company;

— all credit notes, debit notes or other documents which evidence an increase or decrease in consideration that are received and copies of all such documents that are issued by the company;

— a copy of certain self-billing agreements;

— where the company is a customer party to certain self-billing agreements, the name, address and VAT registration number of each supplier with whom the company has entered into a self-billing agreement.

(Regulation 31(1) VAT Regulations 1995 as amended by SI 1996/1250 and SI 2003/3220; Paragraph 2.2 VAT Guidance V1-24A).

The tax authority can require additional records to be kept for particular trades, business activities or special schemes (regulation 31(2) VAT Regulations 1995).

The records must be kept for six years (Paragraph 6(3) Schedule 11 VAT Act 1994) although it is possible by agreement with the tax authority for some records to be kept for shorter periods (Paragraph 5 Schedule 37 Finance Act 2008, Paragraph 19.2 VAT Notice 70, Paragraph 5.4 VAT Notice 700/63 and Paragraph 2.4 VAT Notice 700/21).

What are the VAT rules for the electronic storage of incoming and outgoing invoices?

The rules for storage of invoices supplied and received are the same. The rules on electronic invoicing have been implemented by regulation 13A VAT Regulations 1995.

It must be possible to guarantee the authenticity and integrity of the content of source documents throughout the storage period by electronic means and store all data relating to the invoices. The invoices must be stored in a readable format and the invoice information must be readily recreated as at the time of the original transmission. This applies to scanned images of paper documents used and stored as electronic records for VAT purposes. (Paragraph 5.2 VAT Notice 700/63)

The same time periods apply to storage by electronic invoices as to paper invoices i.e. the normal period of six years (although it is possible by tax authority concession to keep some documents for a shorter period).

Do electronic copies of invoices and contracts have the same evidential value as paper documents? Are there any preconditions?

Electronic copies of invoices and contracts have the same evidential value as paper documents.

For corporation tax purposes, a copy of any document forming part of the records is admissible in evidence in any proceedings before the tax authority to the same extent as the records themselves (Paragraph 22(2) Schedule 18 Finance Act 1998).

For VAT purposes, it is up to the issuer whether to issue electronic or paper invoices; however, the electronic document is not treated as a VAT invoice unless both the supplier and the customer are able to guarantee the authenticity of the origin and integrity of the contents by, for example, advanced electronic signature (regulation 13A(2) VAT Regulations 1995). (The supplier and customer must then preserve the means adopted for guaranteeing the authenticity of the origin and integrity of the contents for such time as the invoice is preserved (regulation 13A(4) VAT Regulations 1995)).

How long must documents be stored to cover the most important statutory limitation periods?

The answer to this question depends on the type of documents to be archived. There is no law governing how long general contracts and deeds should be stored for. However, it is important that they be kept for as long as the relevant limitation period for bringing legal action applies. For contracts, the limitation period is six years after performance and for deeds it is 12 years.

More specific legal provisions apply to the storage of specialist documents, including tax documents, employment documents and corporate documents. For example, the Companies Act 2006 has made it compulsory for minutes of board meetings and shareholder meetings to be stored for ten years.

Many of the longest storage requirements apply in respect of health and safety records. The law states that medical reports must be retained for 40 years. One reason for this is that certain diseases, including those that are asbestos-related, may not be detected for a number of years after the wrongful action. In such cases there is no limitation period for bringing a legal claim therefore long-term storage is necessary.

Do the electronic copies need to be stored at the premises of the company? If not, are data centres in the same country, another EU country or a non-EU country allowed to store them?

There is no general legal requirement for non-personal information to be archived on company premises or within the EEA.

As regards personal information, any transfer of personal data out of the European Economic Area (EEA) must comply with the requirements of principle eight of the DPA that personal data must not be transferred to a country or territory outside of the EEA unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

For tax purposes, there is no requirement for electronic copies of documents to be stored inside the UK for corporation tax purposes.

For VAT purposes, electronic invoices may be stored in another EU Member State (so long as records can be produced in a readable form within a reasonable period of time at a place agreed with the tax authority) and online access to such records is advised. The authenticity and integrity of such invoices must be protected. Electronic invoices may be stored outside the EU provided that the country where the records are stored respects European Data Protection principles and records can be produced in a readable form within a reasonable period of time at a place agreed with the tax authority. Again, online access to such records is advised. (Paragraphs 4.8, 5.5 and 5.6 VAT Notice 700/63).

Must special measures be taken to ensure data security?

In relation to confidential information that is not personal information, where a duty of confidentiality exists the person who owes such a duty is obliged to exercise reasonable care to protect the information from disclosure.

As regards personal data, the law requires that the data controller must take appropriate security measures to protect personal data, taking into account cost and available technology. New regulations are expected in April 2010 which will allow the Information Commissioner to impose fines of up to GBP 500,000 on data controllers who seriously breach this principle (or any of the other data protection principles). The consequences of adverse publicity may be equally costly.

Must special measures be taken to protect the data subjects' privacy?

The DPA provides that personal data should only be stored for as long as necessary to fulfil the specific purpose for which the data is being processed. Once such purpose has been fulfilled, such data should not be retained unless it can be completely anonymised.

The other data processing principles under the DPA of particular relevance to archiving are that personal data must be adequate, relevant and not excessive for the purposes for which they are to be processed, accurate and, where necessary, kept up to date and that appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction and damage. To ensure an equivalent level of data protection for the individual to that available in the EEA, the eighth data protection principle restricts the transfer of personal data to countries outside of the EEA.

The DPA imposes stricter rules for "sensitive personal data" which includes any information related to racial or ethnic origin, criminal records, religious beliefs and health. In many cases, it is not legally possible to process this type of information without first obtaining the explicit consent of the person to whom it relates. It is also important to know that once a person has given consent they are entitled to withdraw it at any time.

Additional obligations in relation to personal information may apply at common law to protect the rights of individuals to privacy. This is a developing area of the law derived from Article 8 of the European Convention on Human Rights.

List of Offices

AUSTRIA
Vienna
CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH
Ebendorferstrasse 3
1010 Vienna, Austria
T +43 1 404 43-0
F +43 1 404 43-90000

BELGIUM
Antwerp
CMS DeBacker
Amerikalei 92
2000 Antwerp, Belgium
T +32 3 206 01-40
F +32 3 206 01-50

Brussels
CMS DeBacker
Chaussée de La Hulpe 178
1170 Brussels, Belgium
T +32 2 743 69-00
F +32 2 743 69-01

Brussels
CMS Derks Star Busmann
CMS EU Law Office
Avenue des Nerviens 85
1040 Brussels, Belgium
T +32 2 65 00-450
F +32 2 65 00-459

Brussels
CMS Hasche Sigle
CMS EU Law Office
Avenue des Nerviens 85
1040 Brussels, Belgium
T +32 2 65 00-420
F +32 2 65 00-422

BULGARIA
Sofia
Pavlov and Partners Law Firm in cooperation with CMS Reich-Rohrwig Hainz
Landmark Centre
14 Tzar Osvoboditel Blvd.
1000 Sofia, Bulgaria
T +359 2 921 99-21
F +359 2 921 99-29

Sofia
Petkova & Sirleshtov Law Office in cooperation with CMS Cameron McKenna
Landmark Centre
14 Tzar Osvoboditel Blvd.
1000 Sofia, Bulgaria
T +359 2 921 99-10
F +359 2 921 99-19

CROATIA
Zagreb
CMS Reich-Rohrwig Hainz
Ilica 1
10000 Zagreb, Croatia
T +385 1 48 25-600
F +385 1 48 25-601

FRANCE
Lyon
CMS Bureau Francis Lefebvre Lyon
174, rue de Créqui
69003 Lyon, France
T +33 4 78 95 47 99
F +33 4 72 61 84 27

Paris
CMS Bureau Francis Lefebvre
1–3, villa Emile Bergerat
92522 Neuilly-sur-Seine Cedex, France
T +33 1 47 38-5500
F +33 1 47 38-5555

Strasbourg
CMS Bureau Francis Lefebvre
1, rue du Maréchal Joffre
67000 Strasbourg, France
T +33 3 90 22 14 20
F +33 3 88 22 02 44

GERMANY

Berlin
CMS Hasche Sigle
Lennéstrasse 7
10785 Berlin, Germany
T +49 30 203 60-0
F +49 30 203 60-2000

Cologne
CMS Hasche Sigle
Kranhaus 1
Im Zollhafen 18
50678 Cologne, Germany
T +49 221 77 16-0
F +49 221 77 16-110

Dresden
CMS Hasche Sigle
An der Dreikönigskirche 10
01097 Dresden, Germany
T +49 351 82 64-40
F +49 351 82 64-716

Duesseldorf
CMS Hasche Sigle
Breite Strasse 3
40213 Duesseldorf, Germany
T +49 211 49 34-0
F +49 211 49 34-120

Frankfurt
CMS Hasche Sigle
Barckhausstrasse 12–16
60325 Frankfurt, Germany
T +49 69 717 01-0
F +49 69 717 01-40410

Hamburg
CMS Hasche Sigle
Stadthausbrücke 1–3
20355 Hamburg, Germany
T +49 40 376 30-0
F +49 40 376 30-40600

Leipzig
CMS Hasche Sigle
Augustusplatz 9
04109 Leipzig, Germany
T +49 341 216 72-0
F +49 341 216 72-33

Munich
CMS Hasche Sigle
Nymphenburger Straße 12
80335 München, Germany
T +49 89 238 07-0
F +49 89 238 07-40110

Stuttgart
CMS Hasche Sigle
Schöttlestrasse 8
70597 Stuttgart, Germany
T +49 711 97 64-0
F +49 711 97 64-900

HUNGARY

Budapest
Ormai és Társai
CMS Cameron McKenna LLP
YBL Palace
Károlyi Mihály utca, 12
1053 Budapest, Hungary
T +36 1 483 48-00
F +36 1 483 48-01

ITALY

Milan
CMS Adonnino Ascoli & Cavasola Scamoni
Via Michelangelo Buonarroti, 39
20145 Milan, Italy
T +39 02 48 01-1171
F +39 02 48 01-2914

Rome
CMS Adonnino Ascoli & Cavasola Scamoni
Via Agostino Depretis, 86
00184 Rome, Italy
T +39 06 47 81-51
F +39 06 48 37-55

THE NETHERLANDS

Amsterdam
CMS Derks Star Busmann
Mondriaantoren – Amstelplein 8A
1096 BC Amsterdam, The Netherlands
T +31 20 301 63-01
F +31 20 301 63-33

POLAND

Warsaw
CMS Cameron McKenna
Dariusz Greszta Spółka Komandytowa
Warsaw Financial Centre
Ul. Emilii Plater 53
00-113 Warsaw, Poland
T +48 22 520 5-555
F +48 22 520 5-556

ROMANIA

Bucharest
CMS Cameron McKenna SCA
S-Park
11–15, Tipografilor Street
B3–B4, 4th Floor
District 1, 013714 Bucharest
Romania
T +40 21 40 73-800
F +40 21 40 73-900

RUSSIA
Moscow
CMS, Russia
Gogolevsky Blvd.,11
119019 Moscow, Russia
T +7 495 786-4000
F +7 495 786-4001

SERBIA
Belgrade
CMS Reich-Rohrwig Hasche Sigle
Cincar Jankova 3
11000 Belgrade, Serbia
T +381 11 320 89 00
F +381 11 303 89 30

SLOVAKIA
Bratislava
Ružička Csekes s.r.o.
in association with members of CMS
Vysoká 2B
811 06 Bratislava
Slovakia
T +421 2 32 33-3444
F +421 2 32 33-3443

SPAIN
Madrid
CMS Albiñana & Suárez de Lezo, S.L.P.
Calle Génova, 27
28004 Madrid, Spain
T +34 91 45 19-300
F +34 91 44 26-045

Marbella
CMS Albiñana & Suárez de Lezo, S.L.P.
Marina Banús, Bloque 4, 15–16
29660 Puerto Banús
Marbella (Málaga), Spain
T +34 952 90 73-20
F +34 952 90 73-19

Seville
CMS Albiñana & Suárez de Lezo, S.L.P.
Avda de la Constitución, 21– 3°
41004 Seville, Spain
T +34 95 42 86-102
F +34 95 42 78-319

UKRAINE
Kyiv
CMS Cameron McKenna LLC
6th Floor, 38 Volodymyrska Street
01034 Kyiv, Ukraine
T +380 44 391 33-77
F +380 44 391 33-88

Kyiv
CMS Derks Star Busmann
6th Floor, 38 Volodymyrska Street
01034 Kyiv, Ukraine
T +380 44 391 33-77
F +380 44 391 33-88

Kyiv
CMS Reich-Rohrwig Hainz TOV
19B Instytutska St.
01021 Kyiv, Ukraine
T +380 44 503 35-46
F +380 44 503 35-49

UNITED KINGDOM
Aberdeen
CMS Cameron McKenna LLP
6 Queens Road
Aberdeen AB15 4ZT, Scotland
T +44 1224 62 20-02
F +44 1224 62 20-66

Bristol
CMS Cameron McKenna LLP
Merchants House North
Wapping Road
Bristol BS1 4RW, England
T +44 1179 30 02 00
F +44 1179 34 93 00

Edinburgh
CMS Cameron McKenna LLP
101 George Street
Edinburgh EH2 3ES, Scotland
T +44 131 220-7676
F +44 131 220-7670

London
CMS Cameron McKenna LLP
Mitre House
160 Aldersgate Street
London EC1A 4DD, England
T +44 20 73 67-3000
F +44 20 73 67-2000

London
CMS Cameron McKenna LLP
100 Leadenhall Street
London EC3A 3BP, England
T +44 20 73 67-3000
F +44 20 73 67-2000


Aberdeen
Edinburgh
Moscow
Hamburg
Amsterdam
Arnhem
Berlin
Warsaw
London
Utrecht
Leipzig
Bristol
Antwerp
Duesseldorf
Dresden
Cologne
Brussels
Frankfurt
Prague
Kyiv
Paris
Strasbourg
Stuttgart
Vienna
Bratislava
Munich
Zurich
Budapest
Lyon
Ljubljana
Zagreb
Milan
Belgrade
Bucharest
Sarajevo
Sofia
Rome
Madrid
Seville
Marbella
Algiers
Casablanca
Beirut
Kuwait City
Dubai
Abu Dhabi
São Paulo
Buenos Aires
Montevideo
Beijing
Shanghai
CMS offices
The members of CMS are in association with the offices of The Levant Lawyers (TLL).