

CEN

CWA 15580

WORKSHOP

July 2006

AGREEMENT

ICS 35.240.99

English version

Storage of Electronic Invoices

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Contents

Contents	2
Foreword	3
Introduction	4
1 Scope	5
2 Abbreviations	6
3 Electronic storage of invoices	7
3.1 Legal environment	7
3.2 Problems in electronic storage of invoices	7
3.3 Service Provider's view	8
3.4 Data from legislation in Member States	8
3.5 Tax audits	9
4 Guidelines for electronic storage of invoices	10
4.1 Legislation on storage – main rules	10
4.2 National legislations	10
4.3 Duration of storage	10
4.4 Place of storage	10
4.5 Storage in the original form	11
4.6 Storage media	11
4.7 Storage of coded data	11
4.8 Storage of digital signatures, long term verification	12
4.8.1 Storage requirements depending on the applied organisational type	12
4.8.2 Facts and recommendations	13
4.9 Technology change during storage period	13
4.10 Terminating the storage service	13
Annexes	14
Annex 1 Organisation Types	14
Annex 2 Results of the questionnaire under section 3.4 on data from legislation in Member States	18

Foreword

This CWA is part of a set of CWAs which has been prepared by the CEN/ISSS Workshop on Interoperability of Electronic Invoices in the European Community, with the view to supporting the effective implementation of the related Council Directive 2001/115/EC of 20 December 2001, with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of Value Added Tax, as well as regulations on electronic signatures and EDI. The set of CWA is as follows:

- Commission Recommendation 1994/820/EC October 1994, proposed revision with the requirements of Directive 2001/115/EC, present day e-Commerce practices and revised definition of EDI Electronic Data Interchange
- The list of invoice content details expressed as UN/CEFACT Core Components
- Recommendation to allow coded identifiers as an alternative to the current unstructured clear text identifications.
- A standardised set of codes with definitions to replace plain text clauses in eInvoice messages.
- Survey of VAT Data Element usage in the Member States and the use of codes for VAT Exemptions.
- eInvoices and digital signatures.
- Storage of Electronic Invoices.
- Guidelines for e-Invoicing service providers.
- eInvoice Reference Model for EU VAT purposes specification

An executive summary of these CWAs is available at:
ftp://ftp.cenorm.be/PUBLIC/e-Invoicing/CWA/Executive_Summary.pdf

This document covers issues on the free choice of the place and method of storage of invoices and the acceptance of electronic storage.

The final review/endorsement round for this CWA was successfully closed on 12 June 2006.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN: AENOR, AFNOR, ASRO, BSI, CSNI, CYS, DIN, DS, ELOT, EVS, IBN, IPQ, IST, LVS, LST, MSA, MSZT, NEN, NSAI, ON, PKN, SEE, SIS, SIST, SFS, SN, SNV, SUTN and UNI.

Introduction

Background

In drafting this CWA, due recognition has been taken of the fact that -

- The provisions of Council Directive 2001/115/EC are applicable to both paper-based and electronic invoicing
- A number of Member States have other national legislation, in addition to Value Added Tax (VAT) legislation, governing the storage of invoices which, furthermore, may be framed according to the specific methods of storage used – e.g. paper, microform, electronic storage
- A number of Member States may require taxable persons to issue invoices, or similar documents, under legislative provisions other than those provided for VAT purposes, under Council Directive 2001/115/EC

This CWA does not cover these issues, but is restricted solely to addressing the provisions of Council Directive 2001/115/EC, with regard to the electronic storage of invoices, by taxable persons or their agents, for VAT purposes.

In this context and for the purposes of this CWA, an “invoice” and a “taxable person” are defined as follows:

Invoice – an application for payment, issued by a taxable person or his agent, in respect of the taxable supply (including Zero Rate) of goods or services. The document evidences the amount of VAT that has been charged by the taxable person and is used to support the recipient’s entitlement to VAT recovery, subject to rules on deductibility.

Taxable Person – a person or organisation who carries on a business that, by virtue of its taxable turnover, is required to be registered for VAT purposes, and who makes taxable supplies for VAT purposes.

Business Rationale

Businesses are increasingly automating their operations and, as a direct result, are implementing the storage of legal documents, including invoices, in electronic form. With electronic storage solutions businesses aim to improve the efficiency of their operations and to reduce costs. Changes to Member States’ legislation are being/have been made to permit the storage of invoices electronically in companies Information Systems (sellers and buyers), or at contracted service providers such as VANs (Value Added Networks), Web services, eInvoice Service Providers or other third parties.

1 Scope

The scope of this document and of the preceding activities, has been to prepare recommended archiving guidelines focused on rules and guidelines for inspection. This also includes rules of the kind of data, and the traceability of commercial operations.

2 Abbreviations

CRL	Certification Revocation List
ES	Electronic Signature
OCSP	Online Certificate Status Protocol
TST	Time Stamp Token

3 Electronic storage of invoices

3.1 Legal environment

Under the provisions of Council Directive 2001/115/EC, regarding the storage of Invoices, every taxable person shall ensure that copies of invoices issued by himself, by his customer or, in his name and on his behalf, by a third party, and all the invoices which he has received, are stored.

The authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed throughout the storage period. With regard to invoices that are not sent under either an advanced electronic signature, or by EDI (i.e. the “third option” – “by other electronic means”), the information they contain may not be altered and must remain legible throughout the aforementioned period.

The taxable person may decide the place of storage, provided that he makes the invoices or information stored there available without undue delay to the competent authorities. Member States may, however, require taxable persons established in their territory to notify them of the place of storage, if it is outside their territory. Member States may, in addition, require taxable persons established in their territory to store, within the country, invoices issued by themselves, or by their customers or, in their name and on their behalf, by a third party, as well as all the invoices which they have received, when the storage is not by electronic means guaranteeing full on-line access to the data concerned. Member States may impose specific conditions prohibiting or restricting the storage of invoices in a country with which no legal instrument exists relating to mutual assistance, similar in scope to that laid down by Directives 76/308/EEC, 77/799/EEC and Council Regulation 218/92 on administrative co-operation in the field of VAT.

Member States shall determine the period for which taxable persons must store invoices relating to goods or services supplied in their territory and invoices received by taxable persons established in their territory.

And finally, Member States may require that invoices be stored in the original form in which they were sent, whether paper or electronic. They may also require that when invoices are stored by electronic means, the data guaranteeing the authenticity of the origin and integrity of the content also be stored.

These provisions are discussed further, under Section 3 below.

3.2 Problems in electronic storage of invoices

The regulations with regard to the storage of electronically exchanged invoices, as indicated in the Directive 2001/115/EC, are not normally an issue where the invoice transaction takes place wholly within a single Member State and the invoice is stored in that Member State. This is due to the fact that both trading partners will be working to the same national regulations and rules.

NOTE However, problems could be experienced by multi-national businesses that operate electronic invoicing domestically (i.e. non-cross-border), in several Member States, in having, as detailed below, to familiarize themselves with the relevant invoice storage legislation that is applicable in each Member State in which they operate.

The main problems are seen to lie with Intra-Community (cross border transactions), where invoicing is from one Member State to another.

This is due principally to the differences in the way that the Directive has been transposed into individual Member State's national legislation; e.g. some Member States stipulate specific formats for storage and/or restrictions as to storage locations, and the required invoice storage period differs from Member State to Member State.

Location and access: The location becomes an issue if invoice storage is in a different Member State to that of where the taxable person is registered. The problem is linked to guaranteeing the origin of the invoices and their integrity, as they may go through several process steps during their end-to-end interchange.

For example, where a company has a central operation (e.g. a Shared Service Centre) for the processing and storage of electronic invoices in respect of its operations in other Member States, invoices will have to be stored in accordance with the regulations in force in each Member State where the company in question is registered. Furthermore, as already indicated, the issues become even more complex if the invoice

documents are to be stored outside the EU community, where Member States may impose additional conditions, or restrict the storage of invoices in a country with which no legal instruments exist for mutual assistance, or, to access the documents on line.

Duration: The question of duration is principally centered on the differences in the number of years that a taxable person has to store invoices, under each Member State's national VAT regulations.

- A multi-country IS will have to store invoices in the system for different periods, depending on the country of issue or receipt of the invoice.
- Where invoices are stored in their EDI syntax format, the relevant directory for decoding the message will also have to be stored for the duration that the invoice is in a coded form. Whilst the storage of documents electronically provides several advantages over paper document storage, such as improved methods of access, control over security, duplication of sensitive documents, etc., it has to be recognised that the rate of change in technology is increasing significantly.
- If documents have to be stored for a period of seven to ten years, there could easily be one or two technology changes during that period, that may present problems in maintaining suitable facilities to preserve the readability of the documents throughout the entire storage period.

Format: The issue of the format of the invoice is closely related to the systems used for transforming the stored data into invoices. Most authorities in the Member States require the invoice data to be presented in a clear format, but do not stipulate how it should be stored.

In some Member States, the invoice data has to be stored in the form in which it has been exchanged e.g. EDIFACT, or paper format, causing companies the requirement to store the data twice.

Medium of storage: The storage medium should not be a problem, since there is a wide range of technical means to meet these specifications.

3.3 Service Provider's view

To collect up-to-date information and to identify the needs from the European service providers' perspective, a questionnaire was designed and implemented in September 2005. The CEN eInvoicing Workshop issued the questionnaire to 101 prospective participants. Altogether, 41 replies were received - the replies provide basic information for all the CWAs in the electronic invoicing area.

Initial findings from the questionnaire are that -

The majority of the respondents (73%) offer an integrated electronic storage service solution for their customers' invoices.

There appear to be sufficient standards or established best practices for electronic storage; only 12,8 % of the respondents wished to have more standards for storage.

The most consistent comments and wishes for storage centre upon legislation. Respondents hoped that invoice storage, in electronic form only, will be made legal throughout the Member States and that when electronic archiving is in use, no paper documents should be required. E.g. scanned paper invoices should be legal archive material EU wide.

3.4 Data from legislation in Member States

For the purpose of collecting up-to-date information on VAT legislation in the different Member States, a questionnaire was designed and sent out to national authorities. Altogether, 22 replies were received. These answers provide important information for the CWAs on invoice storage issues, in the context of VAT and the provisions of Council Directive 2001/115/EC. The results of the questionnaire are presented in a table, as Annex 2 to this CWA.

3.5 Tax audits

It should be noted that electronic storage may also assist tax authorities and auditors. Data can be produced for the auditors for analysis using audit software, or access to the storage can be allowed for tax auditors. The automated audit is more efficient and easier to perform than auditing paper documents. With automated audit tools, data extraction, data analysis, fraud detection and continuous monitoring can be achieved, and the depth and breadth of the analysis improved.

4 Guidelines for electronic storage of invoices

4.1 Legislation on storage – main rules

(*The Italic highlighted text* chapters are direct citations from the directive 2001/115/EC).

The primary rule is that every company, whether the originator or recipient of the invoice, should comply with the legislation in the country where the company is registered.

Secondly, the originator and the recipient are always responsible for complying with the legal requirements for electronic invoicing, even when a third party service is used.

Every taxable person shall ensure that copies of invoices issued by himself, by his customer or, in his name and on his behalf, by a third party, and all the invoices which he has received are stored.

4.2 National legislations

Storage is currently regulated nationally. These regulations differ from Member State to Member State, in terms of e.g.

- what to store
- where to store
- in which format
- for how long
- are there any special requirements and, if so, what are they?

4.3 Duration of storage

The rules covering the invoice storage period vary from Member State to Member State. The disparity can be considerable – e.g. 5+1 years in Denmark and Latvia, and 10+1 years in a number of other Member States e.g. Italy. In certain special cases/for certain invoices, the storage period may be even longer.

The Member States shall determine the period for which taxable persons must store invoices relating to goods or services supplied in their territory and invoices received by taxable persons established in their territory.

In the short to medium term, there is little prospect of Member States reaching agreement on a converged and consistent invoice storage period across the whole of the EU. For a company operating in only one Member State, the current differences in legislation are not an issue.

However, a service provider offering multinational services, or a multinational company's central accounting service, must be ready to meet these different requirements. The simplest solution for service providers is to offer a long storage period, e.g. 11 years for all customers, regardless of their Member State of registration and of the different national regulations that may apply with regard to the storage period.

4.4 Place of storage

The place of storage is considered to be located in the country where the servers used for the storage database are located.

For the purposes of this Directive, the taxable person may decide the place of storage provided that he makes the invoices or information stored there available without undue delay to the competent authorities whenever they so request.

Member States may, however, require taxable persons established in their territory to notify them of the place of storage, if it is outside their territory.

Member States may, in addition, require taxable persons established in their territory to store within the country invoices issued by themselves or by their customers or, in their name and on their behalf, by a third party, as well as all the invoices which they have received, when the storage is not by electronic means guaranteeing full on-line access to the data concerned.

Member States referred to in the fourth subparagraph may impose specific conditions prohibiting or restricting the storage of invoices in a country with which no legal instrument exists relating to mutual assistance similar in scope to that laid down by Directives 76/308/EEC, 77/799/EEC and by Regulation (EEC) No 218/92 and to the right of access by electronic means, download and use referred to in Article 22a.

4.5 Storage in the original form

In order to ensure that the conditions laid down in the third subparagraph are met, Member States referred to in the fourth subparagraph may require that invoices be stored in the original form in which they were sent, whether paper or electronic.

As an opening caveat, there is the need to make the clear distinction between 'form' and 'format'. Form, in the context of Council Directive 2001/115/EC, implies either paper, or electronic. Format has more relevance to electronic invoices, where formats are controlled under standards specifications such as the UN/EDIFACT 'INVOIC' message.

The legislation of some Member States which requires the archiving of paper invoices, in addition to electronic copies, causes companies the problem of double storage, which does not realise the full cost savings that are available through the use of electronic invoicing. Part of these cost savings come from the need not to handle papers, following their scanning, and partly from reductions in storage space requirements. The processes cannot be fully automated, when paper handling remains part of the invoice process.

Some countries also require the original electronic messages to be stored. Again, in this case, double storage is a burden to companies. Auditing e.g. EDI-messages and using the relevant directory for decoding the message, requires a thorough knowledge of the relevant messaging standards. In many countries there is only a requirement to store the data, without any specifications of the data format.

4.6 Storage media

As regards the invoices referred to in the third subparagraph of point (c), the information they contain may not be altered; it must remain legible throughout the aforementioned period.

The integrity of the data on the media for permanent storage must be secured. In order to prevent changes to data, devices like CDR discs may be used, as it is not possible to rewrite the disc. The recording entity can also technically lock a reusable device in such a way that rewriting or adding data is not possible. As an example, the database of the accounting software can be locked after the financial statements have been approved. The database fulfills the requirements for permanent archiving, provided that it is backed-up, on a different medium. Furthermore, it is possible to use methods where a check digit or some other method is used to secure the integrity of the data.

The readability of the storage media must be checked from time to time. If a failure in readability is noticed, a new storage media must be produced without delay.

4.7 Storage of coded data

For storage of coded data please refer to CEN/ISSS CWA on Survey of VAT Data Element usage in the Member States and the use of codes for Exemptions, Reverse Charges, Margin Schemes, etc.

4.8 Storage of digital signatures, long term verification

They may also require that when invoices are stored by electronic means, the data guaranteeing the authenticity of the origin and integrity of the content also be stored.

4.8.1 Storage requirements depending on the applied organisational type

Depending on its organisational trust level a fiscally relevant person, in addition to implement the basic signature verification has to fulfill the requirements detailed in the following table to guarantee the long term validity of the electronic signature. The organisation types are discussed in Annex 1.

Storage Requirements	OL-1	OL-2	OL-3
Basic invoice signature storage	✓	✓	✓
<ul style="list-style-type: none"> ▪ Apply and store TST on the ES; ▪ or countersign the invoice and, if the countersignature does not contain a reliable time reference, apply a TST and store the whole of it ▪ or implement equivalent measures 		✓	✓
Fetch and store certificate path, suitable certificate revocation information for the entire certificate path (CRL/OCSP responses), TST chain, TST certificate path, suitable TST certificate revocation information for the TST certificate path (CRL/OCSP responses)			✓

More in detail:

- where not differently stated by the applicable law, basic Signature verification includes:
 1. cryptographic digital signature correctness,
 2. valid certificate chain;
- organisation belonging to each Organisational Level should, unless differently required by the applicable law, store an ES under its own responsibility to verify the ES validity;
- Organisational Level 2 organisations should additionally, unless differently required by the applicable law:
 1. add a TST (where not already done by the signer) to the signed invoice and store the whole of it;
 2. or, countersign each invoice or a predefined group of invoices and apply a TST to its own signature;
 3. or implement measures officially deemed equivalent to the previous ones;
- Organisational Level 3 organisations should additionally, unless differently required by the applicable law, add to the ES the necessary information to allow for a long term verification, i.e. certificate path, suitable certificate revocation information (CRL/OCSP responses) for each certificate, TST chain, TST certificate path, suitable TST certificate revocation information (CRL/OCSP responses).

In fact, in this case, since no measures exist to protect the recorded invoices from any arbitrary modification, the electronically signed invoices must be intrinsically protected by providing additional information to the electronic signatures. This requires, storing along with the signature (for example in XML data formats):

- a time stamp token issued on the signature the soonest possible, to assert its existence before a certain moment;

- all the involved certificates: all the certificates making up the path from the signer's up to a trust point that can be trusted by any future verifier; the same applies to the Time Stamp Server's certificate and the relevant certification path;
- the revocation information of all the previous certificates, i.e. CRLs and/or OCSP responses, related to a moment, subsequent to the time indicated in the TST, such to allow any revocation request, submitted on the very last moments before the time specified in the TST, to be processed and published by the relevant CA/OCSP Responder; where the same certificate applies to a number of invoices it may be useful to store the related status information only once.

It is to be noted that, in order to have the entire mechanism reliable, the TST issuing organisation may not have lower security measures than those implemented by the invoice-signing certificates issuer.

4.8.2 Facts and recommendations

- Authentication and integrity have to be guaranteed over the whole storage period of invoices.
- Electronic invoicing storing systems need to take that the electronic invoices have to be stored in a way that the electronic signature stays verifiable over years.
- If certain information is not available, to ascertain the certificate revocation status at the time of the signature and a time when the signature itself existed, the electronic signature could not be verifiable in the future.
- Ensuring stored invoices are long term valid, as specified above, depends on both organisational and technical measures- Depending on the trust level of the organisation additional technical measures should be applied.

4.9 Technology change during storage period

The authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed throughout the storage period.

When documents have to be stored over a long period of time, there could easily be several technology changes during that period. In such cases, the taxable person or his service provider must be able to convert the data into another form, when needed, or to retain the hardware/software that will enable the data to be read from the older technology.

Normal backup procedures must be followed for the databases in use. It is possible that permanent storage may be created only once in a fiscal year. Before this, the fiscal data is stored in operational databases, which must also be backed up.

For activities of critical importance, an operational continuity plan must be created. The plan defines the steps necessary to resume critical activities, in the event of an interruption.

4.10 Terminating the storage service

Where the third party terminates the storage service, or the taxable person using the service wishes to terminate the service and remove his data, the third party service provider must assist in moving the data, as necessary, as requested by the taxable person upon termination of the contract.

Furthermore, the third party must store the data in such a way that, upon termination of the contract, it may be moved without disclosure to unauthorised parties and without any other breaches in security.

Finally, the taxable person must ensure that the data is removed and stored, either by himself, or by his new Service Provider.

Annexes

Annex 1 Organisation Types

The organisational requirements to be met, on the basis of the specific Organisational Type, could be defined by the law, where applicable. In this case it would be meaningless to specify here these requirements.

Where no such detail is defined by the law, it is recommended to refer to the ISO 17799: 2005 provisions that cover the main topics hinted to below.

In case of Organisation Type 2 structures, the details on how this standard's provisions are to be implemented will likely be defined by the relevant certification body.

Organisation Type 3 structures are recommended to implement as deep as possible such provisions to prevent being involved in possible future litigations.

In the following paragraphs a synthetical explanation is given of the areas addressed by the mentioned standard that are deemed relevant to invoices issuance and storage and that are deemed as non trivial in the e-Invoicing and storing environment.

1. SECURITY POLICY

It is highly recommended for any organisation involved in IT to establish an Information security policy document as a reference for the entire involved organisation. This document should be submitted to reviews regularly as well as in case of serious security incidents.

Such documents should be consistent with the other ISO 17799 requirements.

2. ORGANIZING INFORMATION SECURITY

a. INTERNAL ORGANIZATION

This would require specific commitment by the Organisation Management to the information security, the details of which can be found in the mentioned ISO 17799:

b. EXTERNAL PARTIES

External parties, be they customers, suppliers or any third party type, should have the related risks identified. From this risk assessment, rules on how to behave when dealing with such external parties would be derived.

3. ASSET MANAGEMENT

This section should address the following areas:

a. RESPONSIBILITY FOR ASSETS

This implies implementing an inventory of sensitive assets (e.g. cryptographic devices, HW and SW used to issue and sign invoices, etc.), explicitly assigning who is the owner (i.e. the person responsible) for each sensitive asset and defining what is the acceptable use of the assets, to prevent misuse and abuse.

b. INFORMATION CLASSIFICATION

Consistently with the previous requirement, assets should be classified according to their sensitivity. This would imply drafting clear classification guidelines, a consistent information labelling mechanism and clear handling instructions.

4. HUMAN RESOURCES SECURITY

The entire organisation reliability depends on its personnel trustworthiness, hence the need to address the security related aspects during the three phases of the relationships between organisation and employees:

a. PRIOR TO EMPLOYMENT

Roles and responsibilities of the organisation management in charge of hiring new employees should be clearly defined, as well as the screening rules, to the extent allowed by the applicable law, and the details of terms and conditions of employment

b. DURING EMPLOYMENT

Although it may appear tautological, it is useful to remember that the organisation's manager roles and responsibilities should be very clearly detailed, to prevent some areas not being addressed or other areas having more than one responsible, thus blurring each manager's duties and responsibilities.

A robust security awareness, education, and training programme should be in place and regularly updated.

Consistently with the applicable law it should be clearly defined what disciplinary measures would be applied when misbehaviour by employees occurs

c. TERMINATION OR CHANGE OF EMPLOYMENT

Job termination is another very sensitive phase of the employment, since quitting employees, even non disgruntled ones, might be a potential source of risk. Therefore a procedure is to be clearly defined assigning the termination responsibilities, how the assets must to be returned, a timely removal of access rights to sensitive information and where necessary how and when these rights are to be changed.

5. PHYSICAL AND ENVIRONMENTAL SECURITY

This topic is often addressed, so a wide knowledge of it is assumed. Therefore the main items addressed by the ISO 17799 are just listed.

a. SECURE AREAS – this will address, according to the single area relevance and sensitivity:

- i. Physical security perimeter
- ii. Physical entry controls
- iii. Securing offices, rooms, and facilities
- iv. Protecting against external and environmental
- v. Working in secure areas
- vi. Public access, delivery, and loading areas

b. EQUIPMENT SECURITY

In addition to the well known issue of "Equipment siting and protection", it is to be remarked that the following issues are to be addressed:

- i. Supporting utilities – it should be planned ahead how to deal with possible disruption or malfunction of electric power and water supply, of sewage disposal problems, etc.
- ii. Cabling security – cables, especially the telecommunication cables, may be subject to eavesdropping, not to mention wireless communication; these possible source of risks must be addressed consistently with the organisation's needs and risk assessment.

- iii. Equipment maintenance – this item should address at least the sensitive equipment maintenance and any maintenance performed by external personnel inside secured areas.
- iv. Security of equipment off-premises – where sensitive equipment (at least) is sent off-premises or regularly operating outside the organisation premises a specific procedure should be drafted indicating how this equipment is to be handled and protected to prevent tampering, damaging, etc.
- v. Secure disposal or re-use of equipment – it too often occurs that equipment, such as a disk, containing gigabytes of sensitive information is disposed of without its content being previously properly zeroised or made really illegible. Specific procedures should indicate how to securely dispose of such equipment.
- vi. Removal of property – in addition to what is specified at the previous item, this one should address also non electronic equipment that might reveal sensitive information.

6. COMMUNICATIONS AND OPERATIONS MANAGEMENT

The most remarkable items addressed by the ISO 17799 are listed.

1. OPERATIONAL PROCEDURES AND RESPONSIBILITIES

In addition to well known items, special attention is to be given to the Separation of development, test, and operational facilities.

This separation does not always occurs: it often happens that operational facilities, especially when implemented by means of redundant instances, are used for the final tests for example by separating the redundant component and using one instance for testing purposes. This can be done only where suitable procedures are enacted that ensure that no “left over” from the testing phase is potentially dangerous, as well as there is a reasonable certainty that the breaking down of the redundant equipment will not affect the operations.

2. ELECTRONIC COMMERCE SERVICES

Its objective is to provide security to the electronic commerce services. This implies that security should be considered, in particular as regards on-line transactions, including integrity and availability of information distributed to the users through systems accessible by external entities.

3. MONITORING

Well known issues are dealt with in this section. Interesting is the “Clock synchronization”, since it implies having a trusted time source available, e.g. a GPS or the like.

7. ACCESS CONTROL

Also this topic is often addressed, so a wide knowledge of it is assumed. Therefore only the more remarkable items addressed by the ISO 17799 are listed.

1. Access control policy

It is recommended to define and clearly document an access control policy that takes into account the actual organisations requirements. It should also be reviewed regularly as well as upon security incidents.

2. Clear desk and clear screen policy

The need for a clean desk policy, as well as a policy to keep the screen clear of information when non attended, goes unmet more often than not, therefore its usefulness is underscored.

3. Sensitive system isolation

ISO 17799 flatly states: “*Sensitive systems should have a dedicated (isolated) computing environment.*” This is a requirement that is well known in the certification authorities environment,

but that would very well apply also to environments dedicated to automatically issuing and storing sensitive documents like e-Invoices, given their fiscal consequences.

4. Mobile computing and teleworking

Although automated e-Invoices issuance and their storage would not likely be of interest to this kind of issue, it is worth mentioning, should any organisation envisage its adoption.

Specific policies are recommended that address this peculiar working situation.

8. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

Also this topic is often addressed, so a wide knowledge of it is assumed.

9. INFORMATION SECURITY INCIDENT MANAGEMENT

Also this topic is often addressed, so a wide knowledge of it is assumed.

10. BUSINESS CONTINUITY MANAGEMENT

Although a wide knowledge of this topic can be assumed, it is useful to remember the importance of setting up a suitable and robust business continuity plan. This is especially true when long term storage is required as in the case of fiscally relevant documents. Therefore a careful planning, testing, re-assessing of the plan is highly recommended, as well as maintaining a single framework of business continuity plans to ensure all plans are consistent.

A special note is to highlight the Business Continuity Plan testing: when such a Plan is to be enacted there is no such thing like a second chance.

11. COMPLIANCE

In addition to the well known topics of "COMPLIANCE WITH LEGAL REQUIREMENTS " and "COMPLIANCE WITH SECURITY POLICIES AND STANDARDS AND TECHNICAL COMPLIANCE", the following one is to be highlighted:

INFORMATION SYSTEMS AUDIT CONSIDERATIONS

This is well clarified by its objective:

"To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

There should be controls to safeguard operational systems and audit tools during information systems audits.

Protection is also required to safeguard the integrity and prevent misuse of audit tools."

Annex 2 Results of the questionnaire under section 3.4 on data from legislation in Member States

	Austria (at)	Belgium (be)	Cyprus (cy)	Czech (cz)	Denmark (dk)	Estonia (ee)
1. Period of storage	in general 7 years, in connection with land related turnover 12 years	7 years	7 years	10 years	5 years	7 years
	Finland (fi)	France (fr)	Greece (gr)	Hungary (hu)	Ireland (ie)	Italy (it)
	6 years from the end of the calendar year during which the accounting period has ended. Concerning invoices received by foreign enterprises this applies only to the invoices received by a fixed establishment located in Finland	6 ans. Les factures informatiques doivent être conservées sur support informatique pendant trois ans, puis sur tout	Until the right of the State to impose tax is statute-barred, usually 5 years or 10 years in case that "fake" invoices exist, i.e. invoices that have not been registered with the competent authorities, provided that it is requested by the relevant legislation, or do not represent a real transaction, or the real transaction has taken place between persons other than those shown in the invoice, or one of the persons shown in the invoice does not exist from a tax point of view, i.e. it has not been declared / registered to the competent tax authorities that it will run business.	8 years	6 years (or less if written permission from local Revenue District obtained)	10 years (Article 2220 of the civil code) or even more, until all the assessments for the corresponding tax period are completed (Article 22 of Presidential Decree no. 600 of 1973).
	Latvia (lv)	Lithuania (lt)	Malta (mt)	Netherlands (nl)	Portugal (pt)	Slovak Republic (sk)
	5 Years	10 years	6 years from end of year to which they relate. In the case of capital goods: 6 years from the end of period of reference. In the case of immovable property: the 6 years will run from the end of a 20 year period.	7 years, or less if authorised, for invoices regarding the development and purchase of (new build) real estate the retention period is 10 years	10 years	10 years (all invoices)

	Slovenia (si)	Sweden (se)	UK	Switzerland (ch)		
	10 years, documentation concerning the taxation of immovable property 20 years.	7 years according to the tax legislation and 10 years according to the accounting law.	6 years, or less if authorised.	10 years; 20 years for business documents associated with immovable property (VAT purposes).		
	Austria (at)	Belgium (be)	Cyprus (cy)	Czech (cz)	Denmark (dk)	Estonia (ee)
2. Kind of data	Every entrepreneur who issues invoices has to keep copies of the invoices and every entrepreneur who wants to deduct input VAT has to keep original invoices. E-invoicing: 1) AES (advance e-signature) based on a certificate issued by a certification-service-provider within the meaning of the Austrian Signature Act 2) EDI: with a summary statement submitted on paper or electronically (with AES based on a certificate)	Every taxable person is required to keep copies of all the e-invoices he issued (in the format of issuing) as well as all the e-invoices received (in the original format of reception). Must also be stored : all raw invoicing data leading to the establishment of the e-invoice, the e-invoice in preceding or following in-house-formats and any document relating to the transfer of e-invoices (eg. acknowledgment of reception)	Persons registered for VAT are required to keep copies of all invoices they issue and all the invoices they receive. They are also required to keep registers of particulars for invoices for purchases and sales.	Taxpayers are required to keep all invoices (or their copies) relevant for tax assessment.	VAT-registered businesses are required to keep copies of all invoices issued and all invoices received. These can be either the message used in data communication, or a document created from that data.	VAT registered persons are required to keep copies of invoices issued by or on behalf the person and invoices for goods acquired or services received by or on behalf of the person . The information set out in an invoice shall be preserved in its original form.

	Finland (fi)	France (fr)	Greece (gr)	Hungary (hu)	Ireland (ie)	Italy (it)
	Taxable persons who carry out taxable or zero rated business in Finland are required to keep - copies of all invoices issued concerning supplies within the scope of the Finnish VAT Act and- invoices received concerning purchases relating to the taxable or zero rated business A stored e-invoice can be the message used in data communication or a document created from that data.	Signature électronique : les factures, la signature électronique à laquelle elles sont liées et le certificat électronique attaché aux données de vérification de la signature électronique doivent être conservés dans leur contenu originel par l'entreprise chargée de s'assurer qu'une facture est émise et par l'entreprise destinataire. EDI : Les informations émises et reçues doivent être conservées dans leur contenu originel. L'obligation de conservation porte sur l'intégralité du message émis ou reçu.	Entrepreneurs are required to keep both invoices issued and received. The issued invoice data must be digitally signed. Both, the data and the sign must be kept and retain unchanged for the necessary storage period (As it is stated in answer 1).	Economic entities are required to keep copies of all invoices issued and all invoices received.	Every taxable person must retain all books, records and documents relevant to the business....Electronic retention of invoices is only acceptable where they were originally issued electronically. .A taxable person keeping electronic records must retain & store particulars such as details of the form of encryption, electronic signature, etc used and the format in which they are stored and how they can be accessed.	Electronic storage of all invoices issued and received as a static unchangeable file. Electronic invoices sent or delivered on paper can be stored both in paper and electronic form.
	Latvia (lv)	Lithuania (lt)	Malta (mt)	Netherlands (nl)	Portugal (pt)	Slovak Republic (sk)
	VAT-registered businesses are required to keep copies of all invoices issued and all invoices received.	VAT-registered businesses are required to keep copies of all invoices issued and all invoices received.	VAT-registered businesses are required to keep copies of all invoices issued and all invoices received. These can be either the message used in data communication, or a document created from that data.	For both purchase and sales invoice all data elements are to be kept in the format as used by the organisation self including its internal control notes. Purchase invoices are to be kept as they were received. Paper invoices may be converted into an electronic format if and when the completeness and correctness are guaranteed and audit remains possible within a reasonable time. Electronic invoices however in general may not be converted to paper. The organisation must be able to provide the sales invoice data on request.	Taxpayers are required to keep copies and of all the invoices issued and all the invoices received. They also must keep a list of all the invoices issued in a tax period.	Taxpayers are required to keep copies of all invoices issued and originals of all invoices received. Taxable persons who are not taxpayers and legal persons who are not taxable persons are required to keep all invoices received. Any person, who sells a new mean of transport to another Member State of the EU, and any person who purchases a new mean of transport from another Member State of the EU is required to keep the invoice on the sale or purchase of it.

	Slovenia (si)	Sweden (se)	UK	Switzerland (ch)		
	VAT registered businesses are required to store all received and issued invoices, documents on corrections to invoices, export and import documents, financial documents, documents on the basis of which they have granted VAT exemptions.	Copies of all invoices issued and all invoices received must be stored.	VAT-registered businesses are required to keep copies of all invoices issued and all invoices received. These can be either the message used in data communication, or a document created from that data.	Electronic data relevant for tax collection purposes must be stored by the sender and the recipient in the original form in which it was transferred and in its entirety. Storage exclusively in printed form or on micro-film is not permitted.		
	Austria (at)	Belgium (be)	Cyprus (cy)	Czech (cz)	Denmark (dk)	Estonia (ee)
3. Kind of storage: what methods of electronic storage, if any, are not permitted?	None.	None	None.	No other methods than invoices guaranteed by means of electronic signature or EDI are permitted.	None, provided the invoices at any time can be printed in hard copy without any modifications.	None
	Finland (fi)	France (fr)	Greece (gr)	Hungary (hu)	Ireland (ie)	Italy (it)
	None. (The unchangeability and readability of the mandatory data has to be guaranteed).	Cf 1 et 2 ci-dessus.	All methods are permitted (electronic form, CD, micro films etc), provided that the authenticity of the origin and integrity of the invoices, as well as their readability, are guaranteed throughout the storage period.	Accounting documents made out in electronic format shall be retained in electronic format, keeping the requirements of the separate legislation on electronic archives, with sufficient facilities to permit the swift retrieval of all information contained in the original document in a perfectly legible form and to contain safeguards to prevent the stored contents from being manipulated or corrupted.	None	There are no limits as to the kind of storage, as long as the documents are kept in a static and unchangeable form.

	Latvia (lv)	Lithuania (lt)	Malta (mt)	Netherlands (nl)	Portugal (pt)	Slovak Republic (sk)
	None	Taxable persons must store documents in the original form in which they were issued or received, whether paper or electronic. During the period of storage the authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed.	None.	None, as long as any audit is possible within a reasonable timeframe during the period of storage.	None	None.
	Slovenia (si)	Sweden (se)	UK	Switzerland (ch)		
	None, if the following conditions are provided: the data contained in an electronic document or record is accessible and appropriate for subsequent use, the data is stored in the form in which it was formulated, sent or received, it is possible to establish from a stored electronic message where it originates from, to whom it was sent, and the time and place it was sent and received, and to a satisfactory degree, the technology and procedures used prevent the data from being altered or deleted, or there is a sufficiently reliable guarantee as to the inalterability of data or messages.	All kind of electronic storage is permitted as long as it can be secured that the information mentioned in the invoice, is not altered and that the information is legible throughout the storage period.	None.	See question no. 2 above.		

Geographical place of storage						
	Austria (at)	Belgium (be)	Cyprus (cy)	Czech (cz)	Denmark (dk)	Estonia (ee)
4. Is storage of invoices by 3 rd parties allowed?	YES	Yes	Yes.	Yes	Yes.	Yes
If YES, what special conditions, if any, are imposed?	None, provided that the invoices can be produced for inspection, within a reasonable timeframe.	None, except that the 3th party will have to store the invoice issued or received by him in all the different formats he does provide, for internal as well as for external purposes.	If storage is in another member state, then they must be available on line and made available to the Commissioner of VAT within 5 days.	Taxpayers are responsible for their authenticity of the origin and integrity of the content, their readability and are required on request of tax authorities to provide them access without unreasonable delay.	None, provided that the invoices can be produced for inspection, within reasonable timeframe. On the storage outside DK we refer to the answers to Q 5 and 6.	None, provided that the person makes the invoices or information preserved therein immediately available to the tax authority at the latter's request.
	Finland (fi)	France (fr)	Greece (gr)	Hungary (hu)	Ireland (ie)	Italy (it)
	Yes	Oui.	Yes	Yes	Yes	Yes

	No special conditions (according to a general condition invoices have to be produced for inspection)	<p>Précision concernant EDI : lorsqu'une station de dématérialisation est gérée par un prestataire de service, la conservation dans leur contenu originel des informations émises ou reçues doit être assurée séparément pour chaque société dématérialisant ses factures</p>	<p>Conditions: a) Invoices or information stored must be available without undue delay to the competent authorities whenever requested. In case that the storage is by electronic means guaranteeing full on line access to the data concerned, Greek tax authorities have the right to access, download and use the invoices for audit purposes. b) If the data are stored out of Greece, (Member State or not) then the competent tax authorities should be notified. c) When the storage is not by electronic means guaranteeing full on-line access to the data concerned, then the entrepreneur should keep also the invoices on paper. d) When the storage is in a country with which no legal instrument exists relating to mutual assistance similar to that laid down by Directive 76/308/EEC and 77/799/EEC (laws 1402/1983 and 1914/1990) and by Regulation (EEC) No 218/92 as to the right to access data by electronic means, the entrepreneur is obliged to keep also copies of the invoices sent and received on paper in his territory.</p>	None, provided that the invoices can be produced for inspection, within a reasonable timeframe (3 working days).	None, but must be accessible to inspection by a Revenue official at all reasonable times.	The persons storing the documents must guarantee on-line access to their archive, by any mean, at any time and from their premises (where the place of storage is in a Member State other than Italy); they must guarantee integrity and readability of contents all throughout the storage period; they must guarantee that all the documents and data included in their electronic archives are printable and can be transcribed onto other electronic media.
			e) In case that invoices are sent abroad electronically by means of electronic data interchange (EDI), then an additional summary document on paper is necessary, unless copies of the invoices sent are stored.			

	Latvia (lv)	Lithuania (lt)	Malta (mt)	Netherlands (nl)	Portugal (pt)	Slovak Republic (sk)
	No	Yes	Yes.	Yes	Yes	Yes
		None provided that the invoices can be produced for inspection	None.	None, as long as any audit is possible within a reasonable timeframe. The organisation outsourcing the storage remains responsible for the data regardless of its location. The Dutch Tax Administration leaves the responsibility of storage with the business for all regulations (tax and non tax alike). Non compliance could result in the reversal of the burden of proof or in a worst case scenario in a criminal offence.	None, since the invoices can be produced for inspection, within a reasonable time limit.	
	Slovenia (si)	Sweden (se)	UK	Switzerland (ch)		
	Yes	Yes, for eInvoices.	Yes	Yes.		
	None. If invoices are stored outside Slovenia, the general conditions are the same as in answer in point 5 .	The taxable person must notify the authorities of the place of the storage, the eInvoice must be immediately accessible for inspection via electronic means and the invoice can be supplied in printed form upon request.	None, provided that the invoices can be produced for inspection, within a reasonable timeframe. Non-EU 3rd parties need to comply with the EC Data Protection Directive, regarding storage of personal data.	The data relevant for tax collection purposes must be directly accessible by the taxpayer for the duration of the storage period. It must be ensured that this data is readable and digitally analysable without unreasonable delay from a single location on Swiss territory		
	Austria (at)	Belgium (be)	Cyprus (cy)	Czech (cz)	Denmark (dk)	Estonia (ee)
5. is storage of invoices within other EU member states allowed?	YES	Yes	Yes.	Yes	The main rule according to the bookkeeping legislation is that records must be kept in DK, unless if authorised otherwise.	Yes

CWA 15580:2006 (E)

If YES, what special conditions, if any, are imposed?	None, provided that the invoices can be produced for inspection, within a reasonable timeframe.	None, provided that :1° the taxable person concerned does inform the competent VAT-office in advance of his plans to do so and of the place of storage, and 2° from Belgium, an on-line full access of the stored e-invoices can be established.	A taxable person storing invoices in another member state needs to inform the Commissioner of that fact and make those invoices available within 5 working days. Storage in another member state is not allowed if there is no electronic online access to the invoices stored.	Taxpayers are required to announce to tax authorities the place of their storage provided that such place is outside CZ. In case of storage of invoices sent by electronic means taxpayers must ensure for tax authorities the right of access in the real time to the invoices and to the data that guarantee the authenticity of the origin and integrity of the content.	I can be allowed, provided that the invoices can be produced for inspection, within reasonable timeframe, and we are informed about the place of the storage	The taxable person or taxable person with limited liability is required to inform the tax authority about the place at which the invoices are preserved.
	Finland (fi)	France (fr)	Greece (gr)	Hungary (hu)	Ireland (ie)	Italy (it)
	Allowed concerning invoices of foreign taxable persons who do not have a fixed establishment in Finland. Otherwise allowed only if invoices are stored electronically and a full on-line access is guaranteed.	Oui.	Yes.	Yes	Yes	Yes
	See the answer above.	Elles ne peuvent pas être stockées dans un pays non lié à la France par une convention prévoyant une assistance mutuelle ainsi qu'un droit d'accès en ligne, de téléchargement et d'utilisation des données concernées (cf. art.22-3-d, 6° alinéa, de la 6° directive).	See answer under 4.	None, provided that the invoices can be produced for inspection, within a reasonable timeframe	None, but must be accessible to inspection by a Revenue official at all reasonable times.	The persons storing the documents must guarantee on-line access to their archive, by any mean, at any time and from their premises (where the place of storage is in a Member State other than Italy); they must guarantee integrity and readability of contents all throughout the storage period; they must guarantee that all the documents and data included in their electronic archives are printable and can be transcribed onto other electronic media.

	Latvia (lv)	Lithuania (lt)	Malta (mt)	Netherlands (nl)	Portugal (pt)	Slovak Republic (sk)
	No	Yes	Yes.	Yes	Yes	Yes
		None. There is an exception for e-invoices. If they are stored in other EU member state, VAT payers must inform tax administrators about the place of storage.	None, provided that the invoices can be produced for inspection, within a reasonable timeframe.	None, as long as any audit is possible within a reasonable timeframe. The organisation outsourcing the storage remains responsible for the data regardless of its location (during entire the storage period).	None, since the invoices can be produced for inspection, within a reasonable time limit.	
	Slovenia (si)	Sweden (se)	UK	Switzerland (ch)		
	Yes	Yes, for eInvoices.	Yes	Yes.		

	<p>If documentation is stored or maintained abroad, taxpayer must inform the tax authority of this. At the request of the tax authority they must submit documentation to the tax authority in the territory of Slovenia within a deadline and at the location determined by the tax authority. If on the basis of regulations abroad this is not possible, they shall submit authentic copies. If documentation is not kept in the Slovenian language, taxpayer must on the request of the competent tax authority, and in a deadline determined by that authority, submit at their own expense certified translations of the requested documentation. In the event that such persons do not submit the translated document within the prescribed deadline, the tax authority shall order its translation at the taxpayer's expense.</p>	See the answer to question No 4.	None, provided that the invoices can be produced for inspection...etc.	See 2 nd paragraph of no. 4 above.		
	Austria (at)	Belgium (be)	Cyprus (cy)	Czech (cz)	Denmark (dk)	Estonia (ee)
6. Is storage of invoices outside EU member states allowed?	YES	Not, by principle	Storage is not permitted in a third country, unless there is a mutual assistance agreement with that third country. At present there are no such agreements in effect.	Yes	No, except from Norway, Iceland, Greenland and The Faroe Islands	Yes

If YES, what special conditions, if any, are imposed?	None, provided that the invoices can be produced for inspection, within a reasonable timeframe	However, when this is done, the administration will request that a permanent back-up 'd be held in Belgium or in another EU-Member-State, provided that from Belgium, an on-line full access to the stored invoices 'd be made possible	Not applicable	See the conditions in No. 5 above.	I can be allowed, provided that the invoices can be produced for inspection, within reasonable timeframe, and we are informed about the place of the storage	The taxable person or taxable person with limited liability is required to inform the tax authority about the place at which the invoices are preserved.
	Finland (fi)	France (fr)	Greece (gr)	Hungary (hu)	Ireland (ie)	Italy (it)
	Only temporarily	Oui.	Yes	Yes	Yes	Yes
	Invoices issued in other OECD-countries can be stored there temporarily until the time of closing the accounts. Invoices issued in Finland can be transferred to other OECD-countries for keeping and closing the accounts. On permission the temporary storage can take place in other countries too.	Sous les mêmes conditions que décrites à la question 5.	See answer under 4.	None, provided that the invoices can be produced for inspection, within a reasonable timeframe	None, but must be accessible to inspection by a Revenue official at all reasonable times.	There must be some legal instrument for mutual assistance in the field of indirect taxation with the country which is storing the invoices. Moreover, the persons storing the documents must guarantee on-line access to their archive, by any mean, at any time and from their premises (where the place of storage is in a Member State other than Italy); they must guarantee integrity and readability of contents all throughout the storage period; they must guarantee that all the documents and data included in their electronic archives are printable and can be transcribed onto other electronic media.
	Latvia (lv)	Lithuania (lt)	Malta (mt)	Netherlands (nl)	Portugal (pt)	Slovak Republic (sk)
	No	Yes	Yes.	Yes	Yes	Yes

CWA 15580:2006 (E)

		VAT invoices documenting supply of goods and services within the territory of the country as well as VAT invoices and other related data received by taxable persons of the Republic of Lithuania may not be stored in territories where Council Directive of 15 March 1976 on Mutual Assistance for the Recovery of Claims Resulting from Operations Forming Part of the System of Financing the European Agricultural Guidance and Guarantee Fund and of the Agricultural Levies and Customs Duties and Council Regulation (EC) No 1798/2003 of 7 October 2003 on Administration of Cooperation in the Field of Value Added Tax do not apply.	None; they must be produced for tracing operations.	None, as long as any audit is possible within a reasonable timeframe. The organisation outsourcing the storage remains responsible for the data regardless of its location (during entire the storage period)..	Storage of invoices outside the EU is subject to a previous authorization by the tax administration, that can require, in a case by case basis, specific conditions to assure that the storage data is kept in integrity and the access to it by the inspection units is easily done.	
	Slovenia (si)	Sweden (se)	UK	Switzerland (ch)		
	Yes	Yes, for eInvoices	Yes	Yes		
	The general conditions are the same as in answer in point 5 .	See the answer to question No 4. It is only possible to store eInvoices in countries with which there exists a legal instrument relating to mutual assistance similar in scope to that laid down by Directives 76/308/EEC, 77/799/EEC and by regulation (EEC) No 218/92.	None, provided that the invoices can be produced for inspection...etc. EC Data Protection Directive, requirements need to be met, re. personal data.	Same requirements as mentioned in question no. 4.		

Traceability of commercial operations						
	Austria (at)	Belgium (be)	Cyprus (cy)	Czech (cz)	Denmark (dk)	Estonia (ee)
7. Are there special requirements for indexing or search possibilities?		No	No	No	No	No
	Finland (fi)	France (fr)	Greece (gr)	Hungary (hu)	Ireland (ie)	Italy (it)
	No	Non.	No	The economic entity shall put the reference to the bookkeeping accounts concerned and the date and verification of entry into bookkeeping accounts on the accounting documents.	No	In accordance with the Ministerial Decree of 23rd January 2004, the process of storing data on appropriate electronic media must make the invoices searchable according to the surname, name, company title, tax identification number, VAT registration number, date, as well as guaranteeing logical associations among the various documents stored digitally.

	Latvia (lv)	Lithuania (lt)	Malta (mt)	Netherlands (nl)	Portugal (pt)	Slovak Republic (sk)
	No	No	No.	No, as long as any audit is possible within a reasonable timeframe and with the same level of service the organisation demands in its own day-to-day handling. Regarding this question it would usually mean that the organisations own audit trail method would/should be sufficient to find any invoice. Common search pattern are the invoice number, the suppliers, the purchase order number of the organisation. Would no search possibility be present this would normally result in a judgement that the organisation lacks auditability in comparison with other organisations with similar type of activity. This could result in the reversal of the burden of proof.	No	No
	Slovenia (si)	Sweden (se)	UK	Switzerland (ch)		
	No	No.	No	Yes, see above.		

	Austria (at)	Belgium (be)	Cyprus (cy)	Czech (cz)	Denmark (dk)	Estonia (ee)
8. Are there requirements for storage of sum or subtotal amounts (tax codes, invoice total, etc.) for the defined period?	Businesses are in general obliged to file preliminary VAT returns electronically with the local tax office on a monthly basis. Preliminary returns may be filed on a quarterly basis if the taxable basis of the taxable transactions did not exceed 22,000€ the previous calendar year.	The periodic VAT declarations (monthly or quarterly) do only summarise the VAT on all invoices issued and all invoices received for that specific tax period (month or trimester)	The amounts of the invoices are only summed up for the purposes of the VAT Account for each VAT quarterly period.	Records should be kept in relation to objective period and VAT stated on invoices should be as well stated at VAT account according to objective period.	Principal summary record is the VAT Account, which summarises the VAT on all invoices issued and all invoices received, for each VAT accounting period (tax period).	Issued and received invoices are recorded in VAT accounts and summarized at the end of the tax period (one month).
	Finland (fi)	France (fr)	Greece (gr)	Hungary (hu)	Ireland (ie)	Italy (it)
	No specific requirements.	Les comptes de TVA retracent l'ensemble de la TVA collectée et déductible telle que mentionnées sur les factures, ainsi que la TVA déclarée pour la période considérée.	Data contained in invoices (VAT is among them) are registered in books and lists, on paper or by electronic means. Periodic VAT declarations (returns) are based on the data registered in the relevant VAT account of the above books and list, from the invoices issued and received. There are specific requirements as to the time for registration, printing etc. of the data registered in books and lists, depending on the way of book keeping, i.e. on paper or electronically.	The economic entity shall retain in a legible form the annual accounts on the financial year, along with the inventory, valuation, the ledger statement and the general ledger and other registers in support of the annual accounts, for a period of at least 10 years.	The VAT control account is the main summary of all invoices for the VAT period for which a return is made.	For each invoice issued/received the following data must be entered in the VAT bought/sold journal: sequential number, date of issue and other elements for identifying the transaction (taxable amount, tax payable, supplier/recipient of the goods or renderer/customer of the service....)

	Latvia (lv)	Lithuania (lt)	Malta (mt)	Netherlands (nl)	Portugal (pt)	Slovak Republic (sk)
	Principal summary record is the account of VAT invoices, which summarises the VAT on all invoices issued and all invoices received, for each VAT accounting period (tax period).	Principal summary record is the register of VAT invoices, which summarises the VAT on all invoices issued and all invoices received, for each VAT accounting period (tax period).	VAT account is to contain all information held for each tax period which is necessary to be furnished in the VAT return for that tax period; it shall also contain any cross references to enable matching and reconciliation of all information contained in it.	No, invoices however are usually processed within (general) ledgers. These ledgers contain both invoice number, net total and VAT amount. (General) ledgers are to be kept as part of the administration of an organisation.	No	

	Slovenia (si)	Sweden (se)	UK	Switzerland (ch)		
	Principal summary record is the VAT Account, which summarises the VAT on all invoices issued and all invoices received, for each VAT accounting period (tax period).	There are no specific requirement for storage of sum or subtotal amounts, but since the accounting law requires storage of all verifications[1], the sums or subtotal amounts can be produced. [1] Invoices are only a part of all the verifications that must be stored.	Principal summary record is the VAT Account, which summarises the VAT on all invoices issued and all invoices received, for each VAT accounting period (tax period).	No, but the data has to be provided in form which enables an automated evaluation.		
	Austria (at)	Belgium (be)	Cyprus (cy)	Czech (cz)	Denmark (dk)	Estonia (ee)
9. Are there additional requirements for storage which have to be fulfilled concerning electronic invoices?	NO	None, provided that they must be stored electronically in such a way that the authenticity of the origin, the integrity of the content and the readability of the e-invoices are guaranteed fully.	When a taxable person provides electronic invoices, that person needs to keep the data used to guarantee authenticity and integrity of the contents for the same period as he keeps the invoices	Electronic invoices can be stored subject to the condition that the method used for transfer from paper to electronic form secure authenticity of the origin, integrity of the content and readability.	Despiction of the system used for registration and storage of invoices.	No

	Finland (fi)	France (fr)	Greece (gr)	Hungary (hu)	Ireland (ie)	Italy (it)
	The data of invoices have to be able to be converted into a clear written form. According to Accounting legislation all accounting material has to be kept on two technical data mediums.	Les assujettis doivent déclarer le lieu de stockage de leurs factures lorsque celui-ci est situé hors de France.	Greek Ministry of Finance has worked out a special technique for invoice data sign, (digital fingerprint of invoice data via SHA-1) that guarantees authenticity of the origin and integrity of the invoices.	Accounting documents made out in electronic format shall be retained in electronic format, keeping the requirements of the separate legislation on electronic archives, with sufficient facilities to permit the swift retrieval of all information contained in the original document in a perfectly legible form and to contain safeguards to prevent the stored contents from being manipulated or corrupted. The taxpayer which issues e-invoices in an EDI network, must have a monthly, paper-based summary document on them.	No	Electronic invoices must be stored at least 15 days from the date of entry in the general accounts by means of electronic signature and time stamping.
	Latvia (lv)	Lithuania (lt)	Malta (mt)	Netherlands (nl)	Portugal (pt)	Slovak Republic (sk)
	No	No	No.	No	No	No
	Slovenia (si)	Sweden (se)	UK	Switzerland (ch)		
	See the answer in point 3.	It must be secured that the content of the invoices is not altered and the information must remain legible throughout the storage period.	No	The data processing procedure applied must provide assurance that all of the data which is to be processed and could be required for tax collection purposes is captured and in addition cannot be suppressed or altered unnoticed.		