Electronic Invoicing - Evidencing a Taxable Supply in the Light of the New VAT Directive

Anna Nordén

1 Background

In December 2001 the European Union Council adopted a directive ("the Invoicing Directive")[1] with the aim to simplify and harmonize VAT invoicing while catering for modern invoicing technologies. The Invoicing Directive introduced important new rules on invoicing generally and regarding electronic invoicing in particular. The aim was that e-invoicing was to be accepted in all Member States provided the authenticity and integrity of the invoice could be guaranteed. According to the Invoicing Directive these requirements could be met by use of advanced electronic signatures (at Member States' choice based on qualified certificates), or Electronic Data Interchange (EDI) where the interchange agreement provided for adequate security procedures. A carve-out provision further allowed Member States to accept "other means" of e-invoicing. The transposition of the Invoicing Directive led to different auditability requirements in the Member States, which has been seen as creating obstacles to the take-up of e-invoicing.

After evaluating the effect of the Invoicing Directive on electronic invoicing, the European Commission in March 2009 put forward a proposal for a new directive, aiming for further harmonization and more freedom regarding measures to evidence an invoice's authenticity and integrity.

2 The New VAT Directive

As of 1 January 2013 companies will have more choice as to how they prove the authenticity and integrity of electronic invoices. This is due to a new VAT Directive expected to be finally adopted in June 2010 (the Directive)[2].[3] An electronic invoice will be defined as an invoice that is issued and received in electronic format. Proof of integrity and authenticity of an invoice (paper or electronic) must be available from the issuance of the invoice until the end of the archiving period. The new Directive makes a clearer distinction than the previous Invoicing Directive between (1) the requirements on the invoice as a discrete object and (2) the objective of those requirements (verifying that a supply actually took place).

---

1 Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax, now merged into the VAT Directive (2006/112/EC).

2 Proposal for a Council Directive amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing, 5985/09 FISC 13 - COM(2009) 21 final.

3 A proposal for a Council Directive amending Directive 2006/112/EC was put forward in March 2009 by the European Commission. This proposal has been negotiated among Member States and a heavily modified proposal was sent to Parliament for advice by the European Council (ECOFIN) in March 2010. After the European Parliament's advisory opinion, ECOFIN is expected to finally adopt the new Directive in June 2010. This article works from the assumption that the ECOFIN decision of March 2010 will be adopted in June 2010.

The new Directive states that an invoice is de facto compliant if a taxable person can prove an actual sales transaction "through business controls establishing a reliable audit trail between an invoice and a supply". In addition to giving companies this option, the Directive maintains the two technical methods from the previous Invoicing Directive as examples of how to ensure the integrity and authenticity of an electronic invoice: electronic signatures and secure EDI.

Member States continue to have the ability to require that the information used to prove integrity and authenticity of electronic invoices also be stored electronically; this option takes on more importance now that the "business controls" method is available to prove the veracity of an invoice on the basis of additional transaction records evidencing a supply.

The new Directive gives the transacting parties a greater freedom of choice, but also creates a need for them to objectively evaluate their different options. This article aims to look at evidence issues and the parties' different possibilities to prove a supply, in the light of the new VAT Directive.

Tax audits are a prime example of business circumstances where it is important to maintain proof that a record (stored data relating to a historical event) is trustworthy. This article takes a tax audit perspective and explores commonly held views on the trustworthiness of electronic records including re-discussing the evidence aspects of the paper and electronic record.

3 The Need to Establish a Supply

3.1 The Role of the Invoice

A tax auditor who is not or only partially privy to the context in which a certain set of records were created needs to establish whether certain historical sales/purchase transactions ("supplies") have actually taken place and that legal obligations as regards calculating tax and presence of certain data are complied with. An auditor must always make a judgment as to the trustworthiness of data: are these the original records exchanged at the time of the supply or have they been fraudulently created or modified? This question is related to the question of 'originality' of data. (Naturally, a tax auditor may not always specifically investigate the trustworthiness of records presented and for example focus only on appropriate tax treatment; this article works from the assumption that the audit seeks to ascertain that records are trustworthy).

The primary record of interest in this context is the invoice, which due to legal requirements and its role represents the most frequent lowest common denominator of explicit (non-oral) data exchange between the trading partners. In a VAT context, "the function of the invoice is to ensure that the right amount of tax is charged for in a supply and it constitutes one of the key elements for audits, in which correct application of VAT provisions is verified".[4] In most countries with VAT, the supplier is explicitly obligated to issue an invoice with a specific minimum content. Often implicitly, the buyer is held to verify this

4 Marc Joostens, Ine Lejeune, Pieter Breyne, Daniel Evrard, *Global (E-)Invoicing & (E-) Archiving*, PricewaterhouseCoopers (2006), p. 46.

invoice upon receipt and reject it in case of errors. Both parties must store the invoice for a period prescribed by law, during which the invoice must be legible. Both parties must be able to demonstrate the integrity and authenticity of the invoice.

3.2 Concept of Original Invoice

One controversial issue that has been much debated is that of the "original invoice".

The CEN e-Invoicing Compliance Guidelines[5] try to draw a clear line between on the one hand any electronic business document exchanged between trading partners as "the invoice" (regardless of the tax jurisdictions involved, including countries without VAT or similar indirect taxes) and on the other hand the "Tax Invoice", which is the dataset in countries where tax law requires an invoice to be issued. The concept of Tax Invoice was introduced to avoid using the concept "original invoice", which has become controversial due to certain tendencies to transpose paper requirements in a one to one fashion onto electronic invoices.

Interestingly, the concept of an "original" has not been fundamentally challenged to the same extent in the (admittedly short) history of e-commerce law up until now. The widely acclaimed basis for e-commerce legislation worldwide, UNCITRAL's Model Law on Electronic Commerce, for example, focuses on the integrity of the information and its possibility to be presented in its definition of an "original"[6]:

> Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:
>
> a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
>
> b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

Whatever way chosen to deal with the originality issue it is clear that an interpretation that requires there to be only one single instance of an invoice is of

5 The European standards organization CEN has since 2001 worked on a variety of technical and self-regulatory standards for e-invoicing. This work has in recent years increasingly attracted participation from tax administrations. One significant output of the Phase II of the CEN e-invoicing workshop is the CEN e-Invoicing Compliance Guidelines (http://www.e-invoice-gateway.net/knowledgebase/eInvoiceBestPractice). These guidelines are based on a common end-to-end e-invoicing process model, whereby each step is further analyzed in terms of principal risks, requirements and control options. The guidelines can be used by users and services providers as a basis for self-assessment of the control framework in place to ensure tax compliance of their e-invoicing process.

6 *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment,* United Nations 1996, Article 8(1).

course challenging in an electronic environment where copies are made in different network nodes and applications during the processing cycle.

3.3 General Record Keeping Requirements

The complexity of the topic can be demonstrated by the fact that the invoice is, in VAT terms, required at a minimum but not in itself sufficient for proving a supply. In most countries, companies are also required to maintain an orderly and auditable administration, which in practice ordinarily means that companies must meet general requirements under accounting law. These requirements, in turn, often include an obligation to retain all records that may be required to substantiate a company's accounts. Trading partners are not explicitly *obligated t*o exchange formalized trade data (key pre-contractual, contractual and transaction data beyond the invoice), but if they do they should generally store these as well.

3.4 Tax Law Enforcement

The enforcement of tax law, and in particular the way audits are performed, is in nearly all countries a matter of national law without much influence from supranational bodies or processes. Audit practices are significantly influenced by that unique local fabric of law, practice, norms and standards that make it very difficult to judge the true extent of requirements in any country. Since the proof of a VAT compliant process is primarily in the audit, this strong national character of tax audit approaches is and will remain the principal obstacle to meaningful harmonization among EU Member States.

4 The Invoice in Relation to other Transaction Documentation

Often, the question to be resolved by a tax auditor is whether a sales (purchase) transaction (a "supply") actually occurred, in order to verify that a supply was treated correctly from a tax –and in particular a value added tax– perspective and what the principal features of that transaction were. In many countries the importance of the invoice is emphasized in relevant tax legislation and the ultimate data point for a tax auditor. The reason that the invoice is the minimum business record to be retained is that the invoice is the most complete concentrate of tax-relevant information. Whereas the invoice contains information regarding the parties, the supply (nature, place, performance, destination etc), the consideration and the tax, only parts of the same information can be found in one and the same of the other transaction documents such as a purchase order, a delivery note, a bank statement or a contract. If an invoice is trustworthy, this provides an almost complete overview of the supply and, when matched against a company's tax declarations, its correct treatment from a tax perspective. It must however also be realized that an invoice by itself can never conclusively evidence a supply: auditors may therefore always require additional information from a company's administration. If the invoice is not trustworthy, an auditor has no choice but to associate administrative records and audit of a

combination of the company's other business records to achieve the same or a higher level of trustworthiness.

Despite what has been suggested by some voices in the EU e-invoicing debate, the trustworthiness of an invoice as a standalone document is still very relevant. A new Directive could have gone all the way and made the right to a deduction of input VAT conditional upon proof of a supply only. Clearly the Member States collectively were reluctant to go that far. Instead, they require a trustworthy invoice and define trustworthiness of an invoice as either residing in the invoice as an object or the general level of proof –by whatever means– that a supply actually took place.

5 Concept of Trustworthiness

A record is normally considered trustworthy when it can be established that its origin is real (authenticity) and that it has not been modified (integrity). These trust attributes are often said to be interdependent: if the integrity of records cannot be established, they are logically not authentic, and if the authenticity of the data cannot be established their integrity is of no interest. Many different factors can influence the trustworthiness of a record, some of which will be presented below.

5.1 Material vs Formal Trustworthiness

Material trustworthiness refers to data being an accurate record of an event; in a tax context, the concept also often includes the data being complete and (particularly for consumption taxes like VAT) reflecting correct tax decisions. Data can be formally but not materially trustworthy. At least in a tax context, material trustworthiness establishes formal trustworthiness – including when formal trustworthiness cannot be separately established.

5.2 Abstraction from Context and Intrinsic Trust Information

The more data are isolated from their context, the more difficult it becomes to establish their trustworthiness. When data are fully isolated from their context, trustworthiness can never be fully established. Nevertheless, certain intrinsic qualities of the data and their carrier medium may convey a level of trust. Semantic trustworthiness is a function of the internal complexity and in particular the interdependencies among subsets of the data; it is more difficult to fake complex information than simple information. The intrinsic trustworthiness of the carrier medium on which data reside can also assist in establishing trustworthiness; copying data from one carrier medium to another always creates a risk of affecting the trustworthiness of the data itself.

5.3 Authority: Role of Third Parties

There is a growing tendency towards companies outsourcing their e-invoicing (and part or all of their other business processes) to service providers. From an audit perspective, introducing a third party that carries a certain authority and that has certain a reputation and a trusted brand can increase the trustworthiness

of the invoice. Such a third party service provider may have a well-established policy and be audited by independent accounting firms, thereby providing a level of trust.

6 Paper vs Electronic Records

When analyzing the way the law and its enforcement have addressed the transition towards the increased dependency on electronic data, it is of interest to revert to the discussions around paper versus electronic records.

The paper document has a unique intrinsic value: it may have been folded; its acid level may have deteriorated its whiteness; it may show a logotype or use a specific layout, font or have other physical features that enhance its credibility as something that was sent or received, and then stored for a certain amount of time. All in all a paper carries unique features that have historically been considered to be meaningful in determining integrity and authenticity of the information on it.

These inherent physical qualities are not always sufficient from a legal perspective to prove that an invoice is real and has not been changed. In practice the fact is however that –at least until the arrival of high-quality word-processing, graphical software, photocopiers and printers on the mass market– these features of the paper record have enabled tax administrations to manage the fraud risk by awarding paper invoices that meet certain minimum physical criteria a de facto presumption of evidence.

This non-legal aspect of the paper-based VAT system is one of the most interesting aspects of the discussion about e-invoicing in the EU. Tax administrations have of course been very well aware of the legal history in the UN, OECD and EU, which have always recognized that the principal obstacle to giving the same legal status to electronic data is the difficulty in attributing ownership and responsibility to data which can be replaced, changed and copied indefinitely.

Two of the biggest questions in the legal world in the past 25 years have been: (1) medium neutrality (ensuring that electronic data are not discriminated against just because it is electronic); and (2) equivalence (treatment of electronic data on par with paper-based data). The legal and legislative communities have been working on various instruments since the 1980s to resolve these questions. The work has often focused on re-interpreting concepts such as writing, document, record, original and signature. The UN Commission on International Trade Law (UNCITRAL) has taken a leading role in reinterpreting these concepts through globally accepted model laws and guidance materials. Similarly, regional bodies such as the Organization for Economic Co-operation and Development (OECD) and the European Commission (EC) have been active in developing new concepts and regulatory frameworks in this area. The consensus positions developed in these intergovernmental organizations have been followed by the adoption of laws and directives on medium neutrality and equivalence worldwide.

It has not been difficult to write rules to ensure medium neutrality. However, ensuring equivalence is more difficult to achieve as this requires criteria to determine when electronic information is 'good enough'.

As stated in the introduction to the UNCITRAL Model Law on Electronic Commerce[7] a data message cannot be regarded as an equivalent of a paper document in that it is of a different nature and does not necessarily perform all the paper document's functions. To handle the equation the UNCITRAL Model Law on Electronic Commerce introduces the *functional equivalence* approach, whereby an analysis is made of purposes and functions of the paper-based requirement with a view to determining how those purposes or functions could be fulfilled through e-commerce techniques.

The discussions around the functions of paper (in the examples often signed with ink) have often revolved around concepts such as authenticity and integrity of the electronic data. This, in turn, has led to a broad debate about the type of security safeguards that are needed to ensure such protection and discussions about the legal value of electronic data have become intertwined with discussions about IT security.

Many of the legal instruments that have emerged after these discussions favor high-quality electronic signatures over other security mechanisms for creating paper/electronic equivalence because electronic signatures based on PKI (digital signatures) theoretically held the promise of watertight and, above all, easily verifiable integrity and authenticity for electronic data. This general preference for PKI is often expressed in terms of electronic signatures that met certain criteria benefiting from the highest level of recognition – an assumption of equivalence.

While electronic signatures can be used to fulfill the paper functions, the evidence situation in the e-world improves compared to a paper invoice since the integrity and authenticity exceeds the paper's level of proof. This is often seen as a benefit from a security perspective, but it has opened the door for a difficult balancing act in EU VAT law, where it has been argued that the emphasis on improved levels of evidence for an inherently insufficient record –the standalone invoice– is not the right policy direction.

7 The New VAT Directive - Ways to Evidence a Supply by Electronic Records

The new Directive contains an obligation for both parties to ensure the integrity of the contents, the authenticity of origin and the legibility of all invoices (whether paper or electronic).[8] The definition of these attributes has not materially changed with this Directive: "The authenticity of the origin" is defined as the assurance of the identity of the supplier or the issuer of the invoice and "The integrity of the content" shall mean that the content required according to the Directive has not been altered.

7 *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment,* United Nations 1996, p. 21.

8 Article 233.

The new Directive however provides greater freedom for the parties as how to meet those requirements. It will now be established that an invoice is compliant if a taxable person can prove an actual transaction "through business controls establishing a reliable audit trail between an invoice and a supply".

In addition to using business controls the Directive stipulates two examples of other methods that can be used to meet the requirements of integrity and authenticity of electronic invoices: e-signatures or contract-based secure EDI, both following more or less the same formulation as the previous Article 233. The e-signature option refers to the definitions in the Directive on Electronic Signatures[9] whereas the EDI alternative refers to a Commission Recommendation[10] and in addition stipulates that the agreement relating to the exchange should provide for the use of procedures guaranteeing the authenticity and integrity.

7.1 Electronic Signatures

The first of the "technologies that ensure the integrity and authenticity" of the invoice is the electronic signatures option. The basis is an advanced electronic signature as defined in the Directive on Electronic Signatures[11] as an electronic signature that meets the following requirements:

> a) it is uniquely linked to the signatory;
>
> b) it is capable of identifying the signatory;
>
> c) it is created using means that the signatory can maintain under his sole control; and
>
> d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The EU definition of advanced electronic signatures is generally interpreted as policy-based PKI-signatures.

The advanced electronic signature can be used to verify the authenticity and integrity of the invoice from the time of issuance until the end of the storage period; by use of modern signature standards (e.g. CAcES[12] or XAdES[13]) the integrity and authenticity can be long-term evidenced without dependency on the issuing Certification Authority.

The e-signature example given in the new Directive however assumes that the advanced electronic signature is based on a qualified certificate and created

9 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Article 2.

10 Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange, Article 2.

11 Article 2.

12 ETSI TS 101 733 v1.6.3: Electronic Signatures and Infrastructures (ESI);CMS Advanced Electronic Signatures (CAdES).

13 ETSI TS 101 903 v1.2.2: XML Advanced Electronic Signatures (XAdES).

using a secure signature creation device (SSCD). Although not a defined term on directive level, this kind of advanced electronic signature is often referred to as a qualified electronic signature. A qualified certificate is issued under a specific certificate policy with high security requirements for the Certification Authority. An SSCD is a device approved by an EU member state on which the private and public key is securely generated and which is used to apply the signature without the private key being exposed to compromise. Member states are required to maintain supervisory bodies for certification authorities issuing qualified certificates. In practice, additional requirements may apply for both advanced and qualified electronic signatures due to local legal, industrial and other specifics.

7.2 EDI Option

For the second integrity and authenticity securing "technology" the new Directive refers to a definition of Electronic Data Interchange (EDI) from a 1994 Commission Recommendation[14]: *"The electronic transfer, from computer to computer, of commercial and administrative data using an agreed standard to structure an EDI message."*

Although the definition of EDI on country level differs somewhat, the concept of EDI is never defined as a security technology. In modern industry definitions, security is not a necessary component of EDI at all: trading partners may very well have discontinued the Value Added Network (VAN) they originally used for their EDI system and, instead, run the same transactions over the unprotected Internet, while continuing to refer to the system as EDI. Importantly, the fact that a system can legally qualify as EDI says nothing about the guarantees it provides for e-invoice integrity and authenticity.

Once a system is legally qualified as EDI, the Directive (as did the previous Invoicing Directive) therefore requires the interchange agreement (also called trading partner agreement or EDI agreement) to provide "for the use of procedures guaranteeing the authenticity of the origin and integrity of the data." What these procedures should be is not well-defined in most member states. However, tax authorities in a number of countries have expressed their intention to use the EU-defined model EDI agreement as the basis for their assessment, which is also the recommendation given in the CEN Guidelines.[15] Significantly, article 6 of this model EDI agreement states:

> 6.1 The parties undertake to implement and maintain security procedures and measures in order to ensure the protection of EDI messages against the risks of unauthorized access, alteration, delay, destruction or loss.
>
> 6.2. Security procedures and measures include the verification of origin, the verification of integrity, the non-repudiation of origin and receipt and the confidentiality of EDI messages.

14 Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange, Article 2.

15 *CEN e-Invoicing Compliance Guidelines* "www.e-invoice-gateway.net/knowledgebase/eInvoiceBestPractice", p. 34.

> Security procedures and measures for the verification of origin and the verification of integrity, in order to identify the sender of any EDI message and to ascertain that any EDI message received is complete and has not been corrupted, are mandatory for any EDI message.

Traditional EDI systems based on an end-to-end VAN are often considered to meet these requirements. However, systems using the Internet need to replicate the extensive security features. If the system owners do not want to use electronic signatures (which would make the system eligible under the Invoicing Directive's e-signature compliance option) such security will ordinarily be ensured through use of point-to-point security mechanisms. Due to inherent limitations of point-to-point security (most notably, it does not offer durable auditability), systems under the EDI compliance option will generally need to include additional security procedures such as frequent logs, and audits in order to guarantee integrity and authenticity. In addition, without verifiable security on the data level, the archive and processing system will often need to include additional integrity-enhancing features.

Some EU member states (including France, Hungary and Spain) have chosen to implement an option in the 2001 Invoicing Directive to require a summary document on paper[16] in addition to the electronic invoice. Conditions concerning the method, frequency, content and reporting procedures for such summary statements tend to differ among countries. Conditions normally apply (implicitly or explicitly) for the systems generating and storing summary statements to be directly populated from the e-invoicing system.

7.3 Business Controls

The new means provided by the Directive to ensure the authenticity and the Integrity is "by any business controls which create a reliable audit trail between an invoice and a supply".

Based on the legislative history and the text of the new Directive's Article 233, one conclusion is that the term "business controls" designates controls that ensure and record the veracity of the actual sales or purchase transaction being completed. This means that both parties must retain evidence that the goods or services referenced in the invoice have been supplied and paid for, as stated in the invoice, between the named parties. This will require a tax auditor to judge an invoice on the basis of combined historical records about the underlying sales or purchase transaction. More concretely, evidence of such controls will generally be a combination of transaction-specific documents or messages (e.g. contracts or pre-contractual communications, orders, order acknowledgements, shipment data, delivery information, payment information etc) and associated system records (logged approvals, reproducible data matching logic, mapping tables etc). Where process-only components play a significant role in establishing a strong evidence position, it will be necessary to document such controls and maintain this documentation through their evolution through time.

16 In some of these countries, the summary statement may be in electronic format.

Third party audit reports could also play a role in demonstrating the fulfillment of a sales or purchase transaction.

Member States continue to have the ability to require the information used to prove the integrity and authenticity of electronic invoices also to be stored electronically. This option takes on more importance when the invoice is evidenced on the basis of additional transaction records proving a supply, since such additional records would then also have to be electronically stored and accessible for tax audit.

A relating complicating factor when choosing the business control alternative is that use of a service provider for part of the relevant business processes means more difficulty for the auditor to establish the full process.

8 How to Value the Different Options

With this new Directive the parties are given more freedom to prove an electronic invoice; if the integrity and authenticity of the invoice as an object cannot be proven, the business process can be used to achieve this. The need for audit remains and has not decreased, which means that the parties need to carefully consider what option to use, and evaluate the alternatives from an evidence perspective.

While practices may differ among Member States, and while very large companies may benefit from special programs that place the emphasis of control on a different level, it remains true for the vast majority of companies that the main focus in a tax audit will be on the smallest subset of data that contains the necessary information and that is sufficiently trustworthy. If the archive contains an invoice that has been exchanged between the parties and accepted by both parties, this holds much of the information necessary to establish the supply. If this invoice is trustworthy it is in most Member States in practice considered sufficient to prove a supply, if there are no other reasons to suspect fraud.

While other methods are available to achieve the same result or –from a general VAT perspective- even a more comprehensive level of evidence of a supply, it must be concluded that the invoice as an object remains critical for companies to ensure a predictable evidence position. Ensuring the integrity and authenticity of an electronic record is an inherent function of an advanced electronic signature, and also generally recognized by legislators around the world as a reliable way to ensure those functions. The invoice as an object will normally be considered trustworthy if a reliable electronic signature is used. Since tax audits often take place many years after the actual supply, one should take into account the fact that other data constellations to prove the integrity and authenticity of an invoice must be carefully maintained during the storage period if such data-level evidence is not available.

What will be considered a reliable and trustworthy e-signature will still vary between Member States. The fact that the example given in the new Directive includes the use of a qualified certificate and secure signature creation device will likely mean that Member States that today require qualified electronic signatures will continue to award a high level of certainty to such signatures.

Use of an e-signature that is considered sufficiently trustworthy by the relevant tax auditor will lead to a reasonably easy evidence situation, and in turn a less complex audit.

The EDI option in the Directive is an alternative to ensure the integrity and authenticity of the invoice. The interchange agreement must explain what procedures are in place to guarantee the authenticity and integrity of the data. Legally in the EU, security requirements for EDI are at best derived from a non-binding Commission Recommendation. To the extent that security is applied to EDI, much EDI security standards work revolves around the use of Public Key Infrastructure (PKI), however any security technique can be used.

The EDI alternative requires extensive process documentation to establish and back-up trustworthiness of the invoice, which also means that more is required from the auditor. All such records also need to be kept during the full storage period.

If the invoice as such cannot be considered sufficiently trustworthy, the lack of trustworthiness can be made up with by expanding the audit and by proving a reliable audit trail between the invoice and a supply using the business process, which is now explicitly acknowledged by the new Directive. An audit of a combination of the company's other business records can lead to the same or even a higher level of trustworthiness.

The downside of the business controls option is that it comes with considerable storage requirements. The option for Member States to require all information used to prove the integrity and authenticity of e-invoices also to be stored electronically may be used by Member States as a way to further define the "reliable audit trail" option in practice. Also, from an audit perspective, if you need go to other sources, because the invoice is not sufficiently trustworthy, the cost structure of the exercise changes. When an invoice is stored abroad, Member States require remote access to such invoices. This logically means that all information used to prove the integrity and authenticity of an electronic invoice must also be made accessible for such remote audit together with the invoice.

Questions relating to the burden of proof in various stages of tax audit can be expected to take on a greater importance in this context: the Directive text clearly establishes a requirement on taxable persons to demonstrate the trustworthiness of invoices. The same specific requirement does not exist for any other type of trade document or administrative record: hence, the burden of proof as regards additional records will often be considered to be on the tax administration when the latter wishes to review such additional information. However, if the integrity and authenticity of the invoice cannot be established in a standalone manner, and must be established by reference to additional business records, it will often be considered that the burden of proof extends to all such records. This means that businesses do not only have the obligation to provide such specific data as requested by a tax auditor, but rather provide such information as part of a proactive evidence exercise where the taxable person needs to demonstrate the historical veracity of a sales transaction.

Member States have until 1 January 2013 to transpose the new rules. How the only real novelty (the introduction of the concept of business processes which establish a reliable audit trail between invoice and supply) will be

interpreted in practice remains to be seen. It is not unlikely that varying transpositions will follow due to the adjective “reliable” being open to interpretation in different cultural contexts throughout the EU.