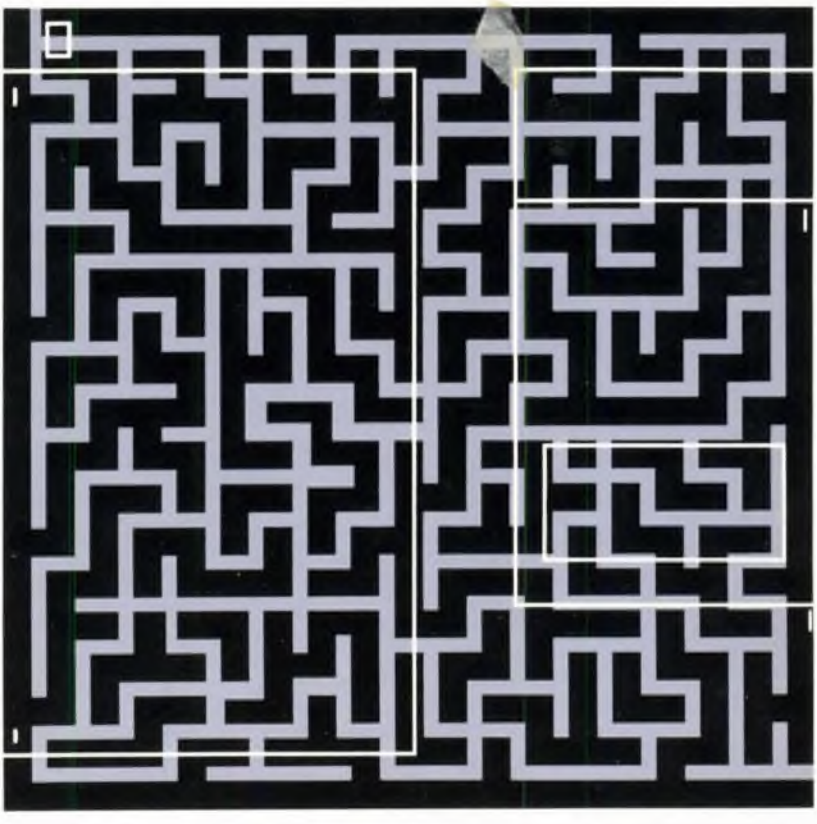
ROLF RIISNÆS

IMPLEMENTING EDI – A PROPOSAL FOR REGULATORY REFORM



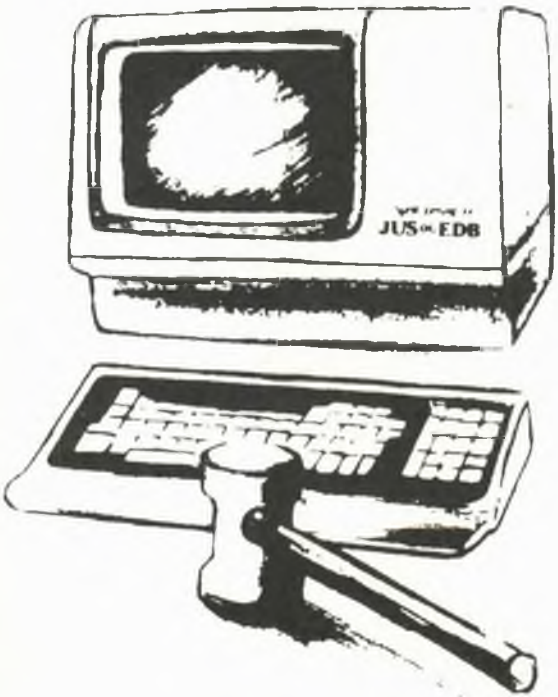
COMPLEX 6/92
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW

TANO

Hovedkontor: Rosenholmvn. 25, 1410 Kolbotn, tlf. (02) 99 80 00
Bergen: Øvre Krakenes 17, tlf. (05) 12 08 00
Stavanger: Professor Olav Hanssens vei 13, tlf. (04) 87 70 00
Trondheim: Vestre Rosten 81, tlf. (07) 88 00 00

Norsk forening for JUS og EDB

Postboks 7557, Skillebekk, OSLO 2
Postgiro 5 13 96 54 Bankgiro 8200.42.49727
Postgiro CompLex 2 12 16 63



Foreningen står bl.a. for salget av CompLex-heftene og vedlikeholder abonnements-ordningene for serien.

WIKBORG, REIN & CO.

ADVOKATFIRMA, M.N.A.

Advokatfirmaet Wikborg, Rein & Co beskjeftiger ca 50 advokater fordelt på kontorer i Oslo, Bergen, London og Kobe Firmaet har spisskompetanse innenfor selskapsrett, skatterett, sjørett, shipping, petroleumsrett, forsikringsrett, finansiering, verdipapir- og børsrett og konkurs- og insolvensbehandling

WR

Sigurd Wælgaard
Erling C. Hjort
Lars A. Christensen
Helge Myhre
Haakon Stang Lund
Einar L. Koefoed
Olav E. Klingenberg
Haakon Blaauw
Tom B. Knudsen
Øystein Meland
John A. Rein
Arne Didrik Kjørnæs

Dag Steinfeld
Stein Pettersen
Knud Lorentzen
Jon Heimset
Christian Friis
Marius M. Gisvold
Trond Eilertsen
Finn Bjørnstad
Lars Olav Askheim
Jan L. Backer
Leif Petter Madsen
Bernhard Haukali
Geir Ove Røberg

Oslo

Kronprinsesse Märthas pl 1
Postboks 1513 Vika
0117 Oslo
Telefon: (02) 33 55 10
Telex: 76131 WRCO N
Telefax:(02) 41 88 22

Bergen

Handelens og Sjøfartens Hus
Olav Kyrres gate 11
5014 Bergen
Telefon: (05) 31 81 16
Telex: 42516 WRCO N
Telefax: (05) 31 00 15

London

1 Knightrider Court
4th floor
London EC4V 5JP
Telefon: (44-71) 236 4598
Telex: 915952 WRCOUK G
Telefax: (44-71) 236 4599

Kobe

1-1, 5-Chome Minatojima
Nakamachi Chuo-Ku,
Kobe 650, Japan
Telefon: (81-78) 303 1772
Telex: 5622404
Telefax: (81-78) 303 1781

CompLex nr. 6/92

Norwegian Research Center for Computers and Law
Niels Juels gate 16
0272 OSLO 2

Rolf Riisnæs

IMPLEMENTING EDI – A PROPOSAL FOR REGULATORY REFORM

TERESA (86)

Developed for the International Chamber of Commerce
under contact with
The Swedish Federation of Industries

TANO

ISBN 82-518-3058-3

Institutt for rettsinformatikks utgivelser i skriftserien CompLex er støttet av:

Den norske Advokatforening
Den norske Bankforening
Digital Equipment Corporation A/S
Lovdata
Norges Forsikringsforbund
Teamco A/S

Fotografisk opptrykk ved
Engers Boktrykkeri A/S, Otta

Foreword

This report has been developed for the work currently being carried out within the framework of the International Chamber of Commerce on electronic data interchange (EDI). It has been contracted by the Swedish Federation of Industries, whose deputy director general, Jan Freese, is chairman for the ICC Working Party on EDI.

Jan Freese approached the Norwegian Research Center for Computers and Law with the idea that a report should be developed which briefly stated typical legal obstacles to the introduction of EDI in national legislation, exemplifying such obstacles with references to or citations from national regulations, and suggesting amendments which would remove the obstacles. This is a rather bold approach, and it is bound to imply simplifications. In other works by the NRCCL, a more traditional and academic approach has been taken.[1] But we were stimulated by the practical thrust of Mr Freese's proposal, and the context in which the work was carried out.

The report has been developed by Rolf Riisnæs in cooperation with Jon Bing. But we have been supported by others at the NRCCL who are working with related issues, especially Olav Torvund and Andreas Galtung.

We would like to thank those mentioned above. In addition, many persons have contributed throughout the process in discussions and correspondence. Not least the staff of Mr Freese has been very helpful.

---

[1] Cf for instance Andreas Galtung, *Paperless Systems and EDI*, CompLex 4/91, Tano, Oslo 1991.

As already stated, this report does not have as its objective to further refine the legal analysis related to EDI. But we hope it may contribute to a structured discussion of the legal policies which may result in a legal environment which will be appropriate for EDI.

Oslo, March 1992

Jon Bing

Rolf Riisnæs

Table of Contents

Introduction

EDI has been defined in many ways. For this report we will, unless stated otherwise, use the definition given in the TEDIS Interchange Agreement, Final Draft of May 1991:

> *Electronic Data Interchange (EDI) is the transmission of data structured according to agreed message standards, between information systems, by electronic means.*

This implies that we deal mainly with the direct, computer-to-computer communication of structured business data, and that the electronic mail systems will be considered here to a small extent only.

As in the TEDIS Interchange Agreement, the term "message" should be interpreted as:

> *A coherent set of data, structured according to agreed message standards, for transmission by electronic means, prepared in a computer-readable format and capable of being automatically and unambiguously processed.*

The aim of this report is not to analyse the legal obstacles to the use of EDI systems, but to work out propositions to solve the problems already pointed out in other reports, such as TEDIS, *The Legal Position of the Member States with Respect to Electronic*

Data Interchange, 1989, and Andreas Galtung, *Paperless Systems and EDI*, CompLex 4/91, Tano, Oslo 1991.

The questions dealt with are, briefly: security aspects, contract formation, accounting and auditing, customs and excise, transport insurance, and evidential questions.

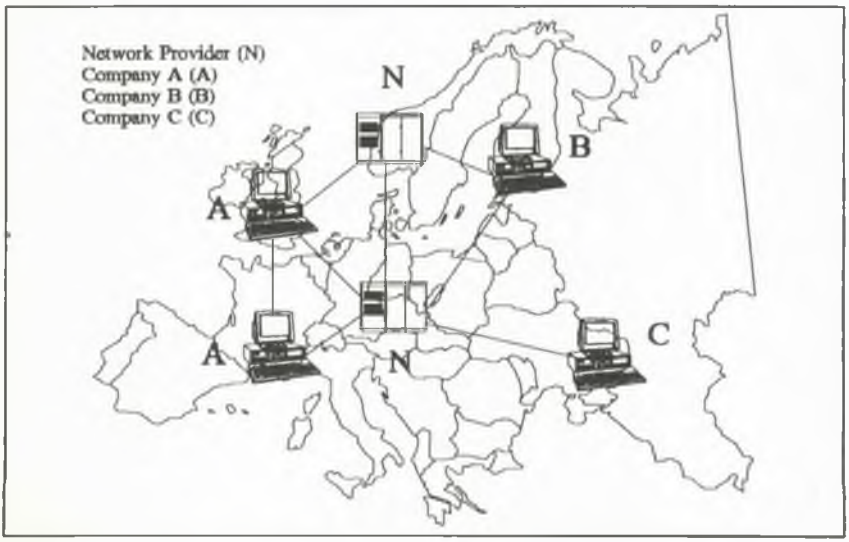
Negotiable instruments, real estate contracts and conveyance of immaterial and intangible assets present common problems in this area. However, it seems that the function of negotiable instruments cannot yet be replaced by electronic means, at least not as a general instrument. The rules being worked out concerning an electronic bill of lading, are not necessarily suitable for other negotiable documents. Transactions involving real estate or intellectual property (copyright, patents, etc) are currently not executed in an EDI environment, and the problems which may arise out of such transactions are not addressed in this paper.

The growing use of EDI may generate problems related to data protection. These issues will not be treated in this report.

Whenever an EDI system is established for the purpose of paperless trading and accounting, a major part of the information needed by the authorities for audit purposes etc will be stored electronically. This solution represents an easier access to a greater deal of information than the traditional paperbased systems. The questions concerning the access of the authorities to such additional information will not be analysed here. Nevertheless, the main principle should be that no external supervisor should have the right to demand access to information which is not necessary to carry out the purpose of the supervision.

The proposals set out in this report are adapted to open network solutions, where the parties are not involved in a prior contractual relationship, and should be regarded as standard terms from which contracts may deviate. In open networks, a contract is entered with the network provider only. The first contact between the seller and the purchaser may be established by computerised means. Whenever a prior framework contract is concluded, the parties may agree on terms different from those set out in this report.

Fig 1: Multinational network with no direct communication between the parties



Additional comments to the report

After the presentation of drafts of the report, some valuable comments have been communicated to us. Some of these have resulted in amendments of the report. Some of them raise issues which we think should be brought to the attention of the ICC working party. These points are summarised below. We emphasise that the issues are characterised as we have understood them and with our own assessment, and may not reflect adequately the points raised by the comments.

1. Could contracts be concluded by EDI?

It has been held that contracts can not be concluded by EDI. We agree that there are some problems regarding the technical solutions for contracting in open networks, but we believe that these problems can be overcome and have retained the discussion in the report.

As to the question of a joint intent between the parties when their systems are concluding contracts, we think this may be solved by system design. The system should contain information on what sorts of goods to sell and buy, and under what circumstances. If the system conclude contracts on different terms than what was expected when the system was designed, this is a risk that the parties involved implicitly have decided to take when engaging in such transactions.

It has also been held that these problems are not present if the parties conclude a framework agreement beforehand. Talking about a corporations main suppliers, one will probably establish such contracts prior to the transaction, but one should not have to do that

with respect to any occasional supplier. We believe that the potential risk of concluding these numerous small day-to-day transactions in an open EDI environment could validly be taken by the parties entering such a system.

2. Revocability - should it be allowed at all?

There are certain problems by allowing revocation of messages made through EDI. If the messages are processed real-time, there will be few possibilities for the revocation to reach the receiver until it is too late, that is when no rule on revocation *re integra* is admissable. Further on, when the messages are being batch-processed, they will be treated sequentially. A message containing a revocation could be "flagged" in such a way that it was given priority, but an advantage of EDI should be that there is no need to know whether your contracting party has a real-time or a batch-processing system. In general, revocation of EDI messages could make problems.

On the other hand, even if the original message is being processed before the revocation arrives, the time gap between them may be so small that the process may be reversable without any economic damage to the recipient. And it would mean major changes *in principle* to the law if one should completely prohibit the possibility of revocation, especially when the *principle of promise* governs the matter.

It should be decided by the ICC whether one should recommend this or not.

3. The credit problem

It has been suggested that evaluation of the credit-rating of a contracting party hardly can be done by computers. This may be so, but again, for all the smaller transactions taking place between occasional parties one have alternatives today. Even if the contracts are concluded and carried through by the EDI systems, we can not see why every part of the transaction should deviate from what is todays common practice. For instance, one may still use the concept of paying cash when the goods are collected or delivered. And finally, automated credit-rating may be difficult and expensive today, but it may be practical with future technology.

4. The battle of forms

The exchange of contractual terms during the process of contract formation is a current problem. Practice proves that the parties, during their day-to-day transactions, assign their standard terms by routine, but to which extent these are accepted by the other party, does not seem to worry them. The suggestion for *EDI-terms* seem to solve some of these problems and, as proposed above, one will probably still negotiate framework agreements with important suppliers. During these negotiations, the subject of contractual terms should be addressed. It has been argued that even *EDI-terms* will not be sufficient, because suppliers like to extend standard terms with their own terms. This may be true. But we do not think it is necessary to solve all the problems of our current situation before adopting a new technical solution. We find that avoiding some of the problems, and not increasing the rest, should be sufficient for a start. We will probably have to learn from experience before we are able to solve all the problems.

5. Computerised evidence in criminal cases

It has been asked whether computerised evidence are sufficient in criminal cases. At this stage we can only recommend that this question should be undertaken an independent study.

Security Aspects

It is necessary to establish some general security requirements for the use of EDI systems. Obviously some transactions require a higher level of security than others, but there are some basic security requirements which may apply generally.

One of the main principles should be to implement measures to avoid transmission errors and unauthorized alteration of the information. Whenever a transmission error occurs, and is disclosed by the recipient, he should notify the sender as soon as possible.

A historical record (log) of the messages being transmitted should be held as long as required by national regulations, or agreements concluded by the party. This may depend on rules concerning the storage of the computerised information based on the messages. If no such requirements are found in the regulations or agreements, the log should be kept for three years. Accounting regulations may be an example of national legislation which may require such documentation to be retained for a longer period. This requirement is justified by control purposes. The choice of a three year period as a default arrangement corresponds to article 10 (c) of the Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission (UNCID).

For the more technical aspects of security standards necessary to comply with these requirements, please refer to:
ISO 9796 Draft International Standard, *Digital Signatures Giving Message Recovery*;
EC - DG XIII, ITSEC, *Information Technology Security Evaluation Criteria*;

and US Department of Defence, TCSEC (the Orange Book), *Trusted Computer Systems Security Evaluation Criteria.*

Basic security requirements should be:

1. *Any party transmitting messages electronically should implement measures to avoid transmission errors and alteration of the data.*

2. *If a message when received appears not to be in good order, correct and complete in form, the recipient should inform the sender thereof as soon as possible.*

3. *A complete historical record (log) should be maintained of all messages as they were sent and received, without any modification.*

4. *The log may be computerised, provided that, if so required, the data can be retrieved and stored in readable form.*

5. *The log should be maintained unaltered and securely, for such time as required by legislation, but for not less than three years.*

Contract Formation

Questions concerning the formation of contracts do not really present legal obstacles to the growing use of EDI systems. One might, however, find that the legal rules governing contracts are not suitable in relation to EDI, and should be replaced.

1. The concept of a document

One basic condition for the use of EDI systems is that no paper is required to establish valid rights and obligations, or to enforce them. This also seems to be the main principle in most jurisdictions regarding the sale of goods. However, there are exceptions. These may refer to transactions of a certain amount, or the requirement for a manual signature. In Belgium and France written evidence is required of agreements involving sums in excess of BF 3,000 (or FF 5,000 respectively)[1], and in the Soviet Union there is a requirement for writing and two signatures for contracts involving parties in other countries. Even if such requirements are subject to numerous exceptions, they should be replaced.

Article 11 (1) of the UN Convention on Contracts for the International Sale of Goods (1980) states:

> *A contract of sale need not be concluded in or evidenced by writing and is not subject to any other requirement as to form. It may be proved by any means, including witnesses.*

---

[1] A consequence of article 1341 of the Civil Code.

The main principle of contract conclusion should be:

> *Contracts can validly be concluded and proven by any means.*

2. When should the offeror be bound by his offer?

The question arises when the principle of promise governs the matter, or the offer is made irrevocable for a period of time.

The Norwegian Contract Formation Act, section 7, states:

> *If an offer or a response to an offer is revoked, the revocation is valid if it reaches the other party before or at the same time that the offer or the answer to the offer has come to his knowledge.*

The Norwegian Contract Formation Act, section 7, implies that the offeror is bound by his offer when it comes to the knowledge of the recipient. This principle applies well to the electronic mail systems, where there must be a human being reading the received mail. However, it does not seem appropriate to the direct, computer-to-computer transfer of structured business data. It does not make sense that something have come to the knowledge of a computer. If one should try to point out at what time the offeror is bound under the current s 7, it must probably be when the offer is registered in the recipient's information system, in such a way that the system can take advantage of the information.

In EDI systems, information is transferred very rapidly. When an offer is sent to another computer, there is no reason for the offeror to believe that he could possibly revoke the offer after it reaches the recipient's information system, but before it is taken further into the system. Due to the speed of the EDI systems one should try to find a point which is easily identified for the purpose of revocability. One such point is the stage at when a message is recorded in the recipient's log. The message will usually get a time stamp at this point. This is also the time when the offer in general is *made available* to the recipient's information system. From this point onwards, it will depend on the circumstances how long it takes until the receiving system takes an action.

For instance: A message is received and recorded in the log. Then it is put in an electronic "mailbox" which is being accessed by a batch process every five or ten minutes. The batch process makes the message available to the relevant part of the information system, but it may take longer before this particular message is interpreted and processed by that part of the system. The legal consequences of receiving a message should therefore, in general, be related to when the message is recorded in the recipient's log. But as discussed below, the message may be considered as made available at an even earlier stage.

Article 15 of the UN Convention on Contracts for the International Sale of Goods (1980) states:

> *(1) An offer becomes effective when it reaches the offeree.*
> *(2) An offer, even if it is irrevocable, may be withdrawn if the withdrawal reaches the offeree before or at the same time as the offer.*

The EDI systems will probably in a few years dominate the markets of international sale of goods. One should, therefore, attempt to introduce uniform rules in this area, even if some countries have not yet adopted Part II of the Convention. The term *reaches the offeree* also seems sufficiently wide to include logging offers into the recipient's system, as such logs should be complete and unchanged trade data records of everything having been received, made at the time of receiving.

A new second paragraph to s 7 of the Norwegian Contract Conclusion Act may be added:

> *If an offer or a response to an offer is transmitted as data structured according to an agreed message standard, between information systems, by electronic means (EDI), it becomes effective when it is made available to the information system of the receiver.*

3. When should the contract be regarded as concluded?

The Norwegian Contract Formation Act, section 7, implies that the contract is concluded when the acceptance reaches the offeror. As proposed above, the term *reaches the offeror* should be read as:

is made available to the recipient's information system.

This point in time is usually easily identified. It also meets the proposition in art 9.2 of the TEDIS Final Draft Interchange Agreement of May 1991 stating:

> *Unless otherwise agreed, a contract made by EDI will be considered to be concluded at the time and the place where the EDI message constituting the acceptance of an offer is made available to the information system of the receiver.*

There do not seem to be any problems relating to the UN Convention. Article 18 (2) of that convention states:

> *An acceptance of an offer becomes effective at the moment the indication of assent reaches the offeror.*

See also UN Convention, article 24:

> *... "reaches" the addressee when it is made orally to him or is delivered by any other means to him personally, to his place of business or mailing address ....*

Article 23 of the UN Convention states:

> *A contract is concluded at the moment when an acceptance of an offer becomes effective in accordance with the provisions of this Convention.*

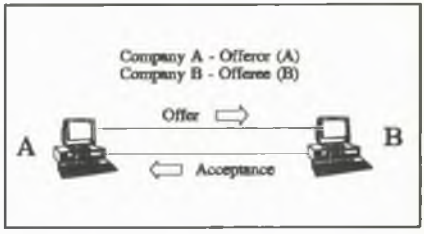
The *postal rule* which is applied in some jurisdictions might apply to the transfer of an acceptance by EDI. The EDI system might be seen as a store and forward system, like the postal service. In that case, the acceptance would become effective at the time it is sent.

The EDI system, however, resembles more an instantaneous system, like the telex systems. The person sending an acceptance via an EDI system does not usually control the transfer. Neither does the offeror. It seems convenient to let each party carry the risk of their own message transmission and not let any message take effect until it is made available to the recipient. Taking advantage of an agreement on *acknowledgement of receipt of EDI messages*, should ensure security and reduce risk to an acceptable level. Such clauses are covered by the TEDIS Interchange Agreement, as well as by the UNCID code of conduct.

4. Where is the contract concluded?

Usually the contract is regarded as concluded at the place where the acceptance becomes effective. This has consequences for the choice of law with respect to the contract. It also shows the importance of introducing uniform rules in this area. Problems may arise in two situations:

Fig 2: The traditional way of offer and acceptance

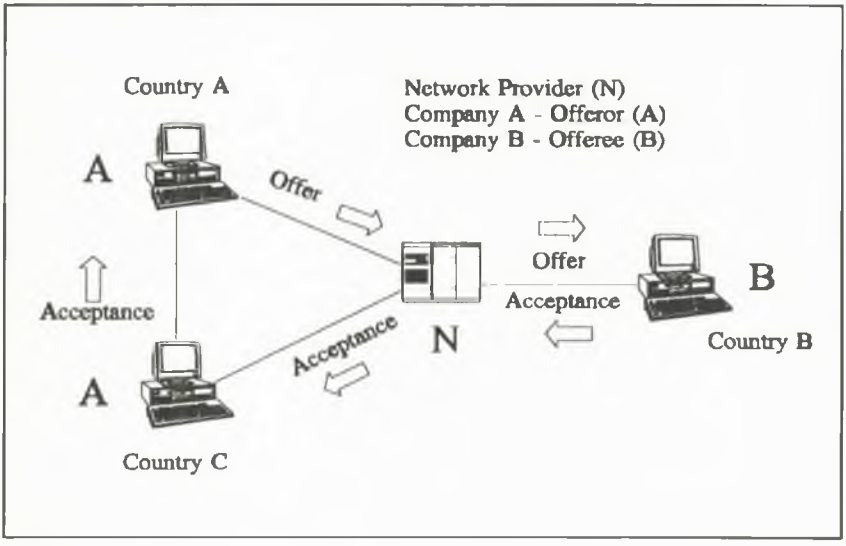


1) The offeror's jurisdiction is governed by the rule that the acceptance becomes effective only when it reaches the offeror, while the offeree's jurisdiction is governed by the postal rule or the declaration rule. What becomes *lex causa* in a dispute on the formation of the contract, if the acceptance never reached the offeror?

2) The acceptance is received by the offeror's computer in a third country, but it is being processed without any delay, in the country

of origin of the offer. Should the contract be considered concluded in the third country, which has no actual interest in the transaction? This problem is likely to become more common with the development of "self-rerouting" networks, where the amount of traffic on the network determines the route taken by the acceptance message - fig 3.

Fig 3: Different routes taken by the offer and the acceptance



It seems that one should emphasise the need for uniform rules in this area. As mentioned before, art 9.2 of the TEDIS Interchange Agreement states:

> *Unless otherwise agreed, a contract made by EDI will be considered to be concluded at the time* ***and the place*** *where the*

EDI message constituting the acceptance of an offer is made ***available*** *to the information system of the receiver.*

The principles of this article should be implemented in national legislation to avoid disputes in this fast growing technique for sale of goods.

One should also consider the consequences of a message being temporarily stored in, or occasionally passing through, a facility controlled by or accessible to the offeror, but different from the facility generating the offer - fig 3. It may be held that the acceptance is *made available* when it reaches a computer or "mailbox" controlled by the offeror, because from this point onwards, it is in the power of the offeror to decide whether he would like to receive the message or not. As distance does not matter in relation to EDI, one could easily think of having "mailboxes" in different places which are being accessed regularly. It would be far too easy to avoid unwanted messages if you could establish such a "mailbox" and then not pick up the messages. In these situations the messages may be considered *made available* at the time and place they reach the sphere of control of the receiver. If this facility is localised in a third country, the contract will be considered concluded in a country with no actual interest in the transaction. In such a case, one should deviate from the main principle and state that the contract is concluded in the country of origin of the offer. This is also the place where the message has to be interpreted and processed.

The statement could be:

> *A contract made by EDI, will be considered to be concluded at the time* ***and the place*** *where the message constituting the acceptance of an offer is made available to the information system of the receiver.*
>
> *If the message is temporarily stored in, or occasionally passes through, a facility in a third country, the location of the information system interpreting and processing the message should be regarded as the place of contract conclusion.*

5. When should an acknowledgement of receipt of EDI messages be made?

EDI systems can be designed to acknowledge receipt of messages automatically, if required. This does not seem to be an expensive or a time consuming function to implement. Neither does it seem to cause any major delays in the system, if it works properly. Moreover, EDI systems for Just-In-Time-Deliveries etc, usually require fast responses.

This implies that the one requesting an acknowledgement, will have reasons to believe that this will be sent without *undue delay*. One could say that it should be sent immediately, and in fully automated systems it probably will. But there will be some systems still requiring human intervention to send such an acknowledgement. The term *undue delay* should cover these situations. If the party requesting an acknowledgement does not know if the system of the recipient is fully automated, he has no reason to believe that the message will be sent until the recipient has had the opportunity to

read the request - maybe he will have to wait until the next workday.

On the other hand, the party receiving such a request should respond as soon as possible. There is nothing to keep the recipient from doing that, as the acknowledgement has no legal implications apart from confirming: "Yes, I have received the message." It says nothing about the content of the message, nor does it commit the recipient to anything mentioned in the message.

The term "without undue delay" should be regarded as a legal standard. The exact time limit in which one should act upon a request for acknowledgement must be decided according to the circumstances of each case. The decision is similar to that of deciding time limits for accepting offers made by telex or cable, and a key phrase might be "as soon as reasonably possible".

There may, however, be a need for a final time limit within which one has to comply with the request. The TEDIS Interchange Agreement holds that, according to EDI experts, one - 1 - business day would be a sufficient period of time for this purpose.

When the parties enter into a prior agreement, they should consider the need for a more specific time limit for acknowledgement of receipt.

6. What should be the consequences of failing to send such an acknowledgement?

If the message requesting an acknowledgement is an offer, failure to respond could imply that the offer is no longer effective. On the other hand, the offeror could state in the offer how long it will stay

open. If no acknowledgement is received, the offer will expire by itself. At the same time, if the offeror receives an acceptance of the offer within the time expected for an acknowledgement, there is no need for an acknowledgement as well.

An acknowledgement of receipt may be more important when the message is an acceptance of an offer, or another kind of message establishing an obligation for the receiver. The sender of such a message may need to know if the message has been received, as otherwise he might have to repeat the message to meet a time limit. In these cases, the immediate response could be of great importance. When the message requesting an acknowledgement is an acceptance or of similar function, the offeror should not be allowed to act upon such a message before giving an acknowledgement.

When a requested acknowledgement is not received within a reasonable period of time, the sender may be required to take action and discover the reason for this failure. On the other hand, this will probably take time. As mentioned before, the sender will not always have the time to comply with such demands. With this in mind, the sender should be allowed the opportunity to be free of whatever rights or obligations his message was intended to establish. He should then notify the receiver of this, because if, for instance, the offeror has sent an acknowledgement that has never reached the offeree, he will need to know if the offeree consider himself free from the implications of the acceptance.

It has been held that most networks provide accurate tracking of messages, and that anyone sending a message should be able to rely on the network's confirmation that the message has been delivered. Further on, the possibility of requesting an acknowledgement of receipt may cause an increase of redundant messages being sent through the system. Nevertheless, apart from what is said about

time limits, etc, any acknowledgement recorded in the log of a party will certainly be considered as evidence in a dispute on whether a message has been received or not.

The rules concerning acknowledgement of receipt should read:

1. *Any party may request the acknowledgement of receipt of the message from the receiver.*

2. *Acknowledgement of receipt should be given without undue delay, and at the latest within one business day following the day of receipt of the message to be acknowledged.*

3. *The receiver of such a request is not entitled to act upon the received message, until an acknowledgement has been given.*

4. *If the message is an offer, the acceptance should also be regarded an acknowledgement, when given without undue delay.*

5. *When the sender does not receive the acknowledgement of receipt within the time limit, he is entitled to consider the message null and void on so advising the receiver.*

Accounting and Auditing

1. Transmission and Storage of Accounting Information

The Norwegian Audit Act of 1977 allows computerised bookkeeping - s 6(5). All costs should be proven by vouchers - s 8, and the vouchers should be kept with the books for at least ten years - s 11.

For the purpose of defining what is accepted as a "voucher" in relation to the Audit Act, additional regulations have been provided.

The so-called *loose leaf* regulations state in s 3 (final paragraph):

> *Accounting documents legitimating the postings could be:*
> 1. *Traditional paperbased documents*
> 2. *Documents on Computer Output Microfilm (COM)*
> 3. *Lists, vouchers, film (COM) etc which are written from received tapes and similar media or by telecommunication*
> 4. .....

There should not be any obstacles towards receiving the vouchers by electronic means - s 3(3)(3).

The problem seems to be that the received data cannot permanently be stored in a computerised form according to the regulations. The received data have to be ***written*** onto another permanent medium to be considered as valid accounting documentation.

This is unnecessary, space-consuming and expensive.

It has been suggested that computerised documents could be manipulated. However, when one allows the vouchers to be received by electronic means, the recipient or any other party who gains control of the data could easily manipulate the data before the voucher is written. These sorts of problems do not really differ from those related to forgery of paperbased documents, and they may be solved by a requirement that logs are to be protected from alteration.

For the purpose of audit trails, the computerised media seem appropriate. They even allow an efficient search of the documents, and making automatic cross-references. This will, of course, depend on the sophistication of the accounting system involved.

To date, one authorisation has been given under the Norwegian regulations to store accounting data in computerised form. The issuing of authorisations on a case-by-case basis does not seem to be appropriate. To avoid the potential problems of computerised storage, one could establish a set of additional requirements - actually not very different from the ones currently being applied.

According to Swedish legislation, accounting information like vouchers may be transmitted by electronic means, as long as the system includes control functions to avoid transmission errors and to ensure that the content of information is not altered. Furthermore, these control functions are to be described in the system documentation, and all messages sent should be recorded in the logs of both parties. These principles are set out by the Swedish official Accounting Committee in their statement *BFN U 89:2*, and are based on ss 5 and 7 of the Accounting Act of 1976:125.

In addition, the statement holds that according to s 10 of the Accounting Act, computerised accounting information may be stored *as long as the general ledger is* ***not*** *computerised.*

In Denmark, new regulations were introduced August 1990. The regulations allow the computerised transmission and storage of accounting data (see Regulations Concerning Business Organisation's Bookkeeping, Annual Accounts and Storage of Accounting Data, 598 of August 21, 1990).

The Norwegian regulations, s 3, final paragraph could read:

> *Accounting documents proving the postings could be:*
>
> .....
>
> 3. *Lists, vouchers, film (COM) etc. which* ***may be written*** *from data received on tapes and similar media or by telecommunication*

This implies that the necessary documentation will come into existence when the data are received and registered by the accounting system.

One should be able to print out the information without any preceding processing. This requirement should be modified to apply over a period of time that is limited to that necessary to secure simple access to the data by any legitimate external supervisor. In Norway, paperbased documentation should be kept for three and a half years for this purpose. After this period the documentation may be transferred to microfilm or other similar media.

In computerised systems the access will be easier. The control functions may also be better, and review will probably take less time than in traditional systems. Moreover, it is expensive to store information in such a way that it can be printed right away. And finally, even if it is not instantaneously printable it may be quicker to generate the information from a computerised system than retrieving paperbased documentation from manual files. Therefore, it might be sufficient to require that the accounting documentation which is stored electronically, should be *printable without preceding processing for one year after the financial year in which registration occurs has expired.* After the termination of this period, the information may be transferred to another permanent medium which secures readability for as long as required by national legislation. This may be for instance five, seven or ten years, but one should consider the cost of storage against the diminished need for control after the first few years. One should also consider the provisions of taxation and prescription regulations. In Denmark the vouchers have to be kept for five years[2], in Sweden for ten.

The question of whether the accounts may be kept in a foreign country will not be addressed here.

2. Information Storage and Security

The issues concerning the preservation of records on computerised media are addressed in the Danish Accounting Regulations and in Luxembourgoise legislation. The main principles of Luxembourg's regulations are presented in the TEDIS report. Some of them will

[2] Section 17(1) of the Danish Accounting Regulations.

Proposed regulations are:

1. *Vouchers proving the accounting may be based on information which has been transmitted by computerised means.*

2. *The vouchers may be computerised.*

3. *The vouchers should be directly printable on paper for one year after the financial year in which registration occurs has expired.*

4. *Readability of the vouchers should be assured for ten years after the financial year in which registration occurs has expired.*

   If the accounting system is being replaced, or for other reasons becomes inaccessible, the vouchers should be printed on paper or transferred to another system or media to secure readability.

be presented here by way of example[3]:

Other than the balance sheet and profit and loss account, all other documents and information required under arts 8 and 10 of the Commercial Code may be preserved on micrographic or electronic media, provided that the reproductions or recordings correspond to the content of the documents or information being preserved; that they be available on a permanent basis for the duration of the

[3] TEDIS report pages 176-178.

preservation period in a directly readable form; and that they satisfy the aforementioned conditions.[4]

The computer-stored information must:

a) be an accurate and durable reproduction or recording of the original document or information forming the basis of the recording;

(The concept of "durable" used here can be applied to any indelible reproduction of the original and any recording which entails an irreversible modification of the input medium.)

b) be recorded in a systematic manner with no omissions;

c) be recorded in concordance with the working instructions which have been preserved for the same amount of time as the reproductions and recordings;

d) be carefully preserved in a systematic way, and protected against any alteration.[5]

The computer program manuals, descriptions and instructions must be directly readable and kept meticulously updated by whoever is in charge of maintaining them.

This material is to be preserved in a communicable form for a period equal to that of the recordings to which they refer.[6]

If, for whatever reason, the recorded data is transferred from one data carrier to another, the official responsible must be able to demonstrate that the two versions are identical.[7]

---

[4] Revised art 11 of Luxembourg's Commercial Code.

[5] Art 1 of the Grand-Ducal Regulation of 22 December 1986, in accordance with art 1341 of the Civil Code.

[6] Art 3 of the Grand-Ducal Regulation of 22 December 1986, in accordance with art 1341 of the Civil Code.

[7] Art 3(2) of the Grand-Ducal Regulation of 22 December 1986.

The computer systems used must provide the necessary security measures to prevent any alteration of the recordings, and allow the stored data to be translated at any time into a directly readable form.[8]

The program used must, furthermore, be compatible with regular accounting procedures.[9]

One of the major points is to store the data unaltered and securely. It is certainly more difficult to protect system data from being altered by its owner than by any outsider, but this problem may be solved by the use of digital signatures and hashing-algorithms for optimalisation purposes.[10]

The records of the log could probably be automatically compared to the electronic archive. This will disclose any changes made to the data after it was received. Forgery of both the log and the archive would not be trivial.

---

[8] Art 9(3)(a) of the Grand-Ducal Regulation of 22 December 1986, in accordance with art 1341 of the Civil Code.

[9] Revised art 11 of Luxembourg's Commercial Code.

[10] An example of this could be the X.509 CCITT standard.

Proposed requirements with regards to information storage are:

5. *The vouchers should:*
   a) *be an accurate and durable reproduction or recording of the messages on which they are based;*
   b) *be recorded in a systematic manner with no omissions;*
   c) *be carefully preserved in a systematic way, and protected against any alteration.*

6. *The log containing the messages on which the vouchers are based should be preserved for a period equal to that of the vouchers.*

Customs and Excise

1. Transmission of Customs Declarations

To ensure the effective transborder trade of goods, which is supported by the use of EDI-systems, it seems to be of great importance that goods flow across borders with a minimum of delay caused by manual routines. One should, therefore, push for the development of paperless systems in customs clearance.

Any legal obstacles to the use of these systems should be removed. In Sweden this has been done recently. The traditional requirement of a signed paper-based customs declaration, has been replaced. In addition to a number of changes in existing regulations, several new sections have been added to the Swedish Customs Act (1987:1065).

The new section 34a specifies:

> *For a payment in accordance with the regulations of sections 25-34, information between the Customs and another party may be given by transmission of an electronic document, according to regulations given by the Government.*

See also the new section 11a which reads:

> *The General Customs Committee may permit that customs declarations and other information which should be given according to this act or the act (1987:1069) on exemption from duty etc, may be provided by an electronic document to the customs data processing system or in another way by automated data processing.*
>
> *An electronic document is considered to be a record, the content and creator of which, should be able to be verified by a certain technical procedure.*
>
> *A permission given under this section may be supplemented with requirements as to the technical procedure for delivery of the information, and as to the procedure in general.*
>
> *The Customs authorities may transmit electronic documents and other information to a declarant through the customs data processing system.*

The legal history of the new regulations are contained in *SOU 1989:20*, *SOU 1990:37* and *Prop 1989/90:40*.

It should be emphasised that for the parties using computerised declarations, the sanctions against violating the rules are not only penalties but the risk of being excluded from the use of the paperless system. The time aspect makes access to these systems of competitive importance. This sanction can probably also be implemented in the interchange agreement. This has been done in the interchange agreement between the Norwegian Customs and declarants.

This customs information interchange agreement reads as follows:

> 1. *The undersigned importer/forwarding agent assumes responsibility for the information transmitted to the Customs, using the identification code given below, with the same effect as if it was signed by him.*
>
> .....
>
> 4. *This permission may be withdrawn without any further warning, if the conditions are not being followed.*

The content of s 4 of the Norwegian Custom's interchange agreement corresponds to clauses in the permissions issued by the Swedish Customs for paperless declarations.

The problems relating to the storage of accounting documentation also apply to the preservation of customs declarations, which may also be considered as accounting documentation. The proposed rules for storage of such documentation should apply correspondingly.

2. Customs Declarations - the Responsibility of the Declarant

A customs declaration is traditionally made by the declarant filling in a form, signing it and sending it to the customs authorities. The declarant will be responsible for any misleading information in the declaration. Should the customs authorities wish to prosecute an importer in a court of law for fraudulent misdeclaration of goods at

importation, a signed customs declaration submitted to the court as evidence would carry considerable weight.

Alternatively, the declaration scheme can be computerised. The declarant sends an electronic message to the customs authorities for the purpose of import or export, and the digital signature may play an important role to authentify the sender.

When the exporting party has sent his declaration electronically to the customs authorities of the exporting country, it seems efficient to transfer this information directly to the customs authorities of the importing country, without having the importing party as an intermediate. That is, of course, subject to an agreement between the exporter and importer. They may, for instance, be companies within a transnational concern, one of them an international supply centre. The problem appears to be that customs declaration is based on the responsibility of the declarant. In this case the relevant importing party has not been directly involved, and it might be difficult to find ways of sanctioning a misdeclaration.

This may be solved by a requirement for the third party generating the declaration to send a copy to the importer. The importer should have the duty to ensure that the declaration is correct and adequate with regards to the goods ordered and expected. This should be done as soon as possible, and if any discrepancy is detected, he should notify the customs authorities of this without undue delay. As long as the notification is made within the stipulated time, the importing party will have the right to alter the declaration sent by the exporting party. Otherwise the importing party will be held responsible for the content of the message.

In any case, there will be a need for an information exchange directly between the customs authorities in different countries in the

EDI system concerning *goods in transit*. Further on, the suggestion above may be useful with respect to the European Communities' future arrangement with so called *authorised traders*.

It seems difficult to apply criminal sanctions to an individual in these situations. But applying such sanctions will probably not be necessary. There may still be the possibility of using economic sanctions towards the importing company, and one could also exclude the importer from the system of electronic declaration. These sanctions can probably even be established by contract. As long as there is an alternative for declaring goods, there will be an economic "risk" which the importer may accept by way of contract. Such sanctions should also be part of the regulations.

The regulations could read:

1. *The information needed for customs declaration purposes could be transmitted by EDI upon permission given by the customs authorities.*

2. *Whenever a customs declaration or any other information needed by the Customs is being transmitted electronically, the sender is responsible as if the message was signed by him manually.*

3. *A customs declaration or other information may be sent directly from the exporting country to the Customs of the importing country.*

   Whenever a declaration is sent directly from the exporting country to the Customs of the importing country, a copy should be sent to the importer who will be regarded as the declarant.

The importer should ensure that the content of the message is correct and adequate with regards to what is ordered and expected.

4. *Whenever a declaration or other customs information is sent pursuant to no 3 above, the importer should notify the Customs whether the content of the information sent is incorrect or incomplete.*

   Such notification should be sent as soon as the importer should be aware of the circumstances causing the notification.

   When such notification is sent, the importer should have the right to alter the information, otherwise he will be held responsible for the content.

5. *The customs authorities may withdraw any permission given pursuant to no 1 above if the regulations are not being followed.*

6. *The information on customs declarations may be stored electronically.*

   The requirements for storage of accounting documentation should apply correspondingly.

Transport Insurance

An issue connected to the increased use of EDI in the international sale of goods is that of transport insurance agreements.

Article 25 of the Belgian Non-Marine Insurance Act of 11 June 1874 provides that the insurance contract must be legally proven by writing regardless of the value of the insured object, although proof by testimony will be admitted if there is *prima facie* evidence in writing.[11]

The requirement for contracts of insurance to be made in writing also applies to Spanish law[12] (see art 5 of Act 50/1980 of 8 October).

When the contract formation, transfer of vouchers, customs declaration and payment are done electronically, it is inconvenient that any insurance contract regarding the transaction should have to be concluded in writing. This will probably cause an unnecessary delay. In any case, the insurance document will usually not be issued until a certain amount of time has gone by; that is, when transport is terminated or damage has occurred. Until then, the insurance is registered only in the insurer's electronic system. Why could it not just stay there?

Even if most companies conclude their open insurance policies, there will still be a need for individual insurances in certain cases. Apart from the ones *not* having an open insurance policy, one has

---

[11] TEDIS report page 97.

[12] TEDIS report page 121.

the need for an insurancce agreement in favour of the receiver of the goods. But as long as the cargo is known, which it certainly will be in an EDI environment, why cannot the insurance simply be registered with the insurance company, so to say *in blanco*, made in favour of anyone entitled to the goods? The cargo could even be tracked down by advising the insurance company whenever the goods are sold while still *in transit*. This could be done automatically.

The transport insurance contracts could probably be standardized to a great extent. If that is the case, they should be suitable for formation by computerised systems.

Section 17-1 of the Norwegian Insurance Contract Act of 16 June 1989, nr 69, states *inter alia*:

> *A life insurance company shall register the insurance contracts it concludes.*

It is not clearly stated that the registration can be computerised, but this is evident from the legislative history. The registration is made in each insurance company. Since this principle is appropriate for life insurance contracts, it should also be appropriate for transport insurance contracts. No paper documents are needed in this respect.

Some additional regulations, however, might be required in connection with the conclusion of insurance contracts.

There will probably be a need to conclude these agreements very quickly. The demand for Just-In-Time-Deliveries will normally not

allow any manual part of the transaction. Neither is it convenient to wait for the confirmation of an insurance agreement. As the insurance agreement could be based upon standard terms, the insurance company should be able to respond very quickly. The insurer offering the computerised conclusion service should therefore be obliged to inform immediately whether the requested insurance will be accepted or not. If the insurer fails to do so, the party requesting the insurance should automatically be free from whatever rights or obligations the request was meant to establish.

The standard terms could be based on a set of codes similar to the Incoterms. The information necessary to conclude a transport insurance agreement is: Location of dispatch and arrival, the kind of goods that are sent, the value of the goods, and the method of shipment.

There are already sets of country codes which may be used for this purpose. Furthermore, the Harmonized System Codes worked out by the Customs Co-operative Council (CCC), and in force since 1988, put goods together in suitable groups. Many corporations have already made these codes part of their article master file for the purpose of paperless customs declaration. The same codes may be used to calculate the insurance rate. There is also a set of Transport Codes worked out by the United Nations Economic Commission for Europe (UNECE) and made part of the paperless customs declaration (CUSDEC) code 8067. These codes seem to cover most needs for insurance rate calculation. By putting these codes together, one may have the basis on which standardised calculation rules may be built.

Proposed outlines for regulating the conclusion of transport insurance contracts are:

1. *Transport insurance agreements may be concluded by messages transmitted electronically.*

2. *The records of such insurance agreements may be stored electronically with the insurer.*

3. *Any insurance company offering the electronic conclusion of transport insurance agreements, should respond immediately to a message requesting such an insurance.*

4. *If the insurer fails to respond to such a message, the party requesting the insurance is entitled to consider the request null and void.*

Evidence

1. Admissibility of Computerised Evidence

It seems that the regular situation in civil law jurisdictions is that in commercial relationships computer-generated or computer-stored data are admissible in courts of law as evidence. In common law jurisdictions the position of such data seems to differ between criminal and civil cases, and between computer-generated and computer-stored material. No matter what, the trend is that computerised data are considered admissible as evidence. This is also a matter of necessity. The rules concerning admissibility might be replaced by rules regarding the strength and burden of proof.

There has been a discussion over whether computer-stored data could be regarded as written evidence. Even if this discussion, *inter alia*, is of importance to whether computer-stored material complies with the requirement of a "best evidence" rule, it does not seem to have any great value. The way to go must be to allow any such material to be used to prove a claim. It should then be up to the court to decide the strength of such evidence. This decision should be based on information about computer security, about the organisation managing the system, on whether the system was working properly, and the system documentation - anything relevant to tell the court whether the computerised evidence should be trusted.

The computerised evidence should be presented to the court in a readable form, but not necessarily in the form of a paperbased document.

2. The Burden of Proof

In general, the burden of proof is on the party making a claim. But from time to time the onus of proof is reversed by law, or by the situation of the actual case. One example will be found in section 22(4) of the Danish Payment Card Act 1984. It states that the card issuer has the burden of proving that any payment transaction did not generate from any kind of misregistration or technical failure, even when the error was occasional. It is quite obvious that it is the card-issuer and not the card holder who is able to establish evidence regarding whether the system was working properly or not.

Based on the same principle, it might be sufficient to place the onus of proof on the party controlling the computer system, or, if the system is controlled by a third party network provider, on any party violating the requirement of keeping a complete and unchanged log, or other security standards. EDI systems are potentially the quickest and the most secure way to exchange information, but it depends on the participants following certain rules, such as the ones set out in the UNCID code of conduct.

An example could be that two parties have chosen to trade by EDI. They are both subject to the requirement of keeping a log. Party A has received an offer from party B, and sends an acceptance to B, but B holds that the acceptance was never received. The log of party A shows that the acceptance was sent. Party B does not have a log as required. In this case, the burden of proof should be upon B to prove that the acceptance was never received, even *if it* normally would be upon A.

The regulations could read:

1. *Any computer-generated document, message or other such data items received or stored electronically are admissible as evidence.*

2. *The electronic document must be presented to the court in readable form.*

3. *Any consideration regarding the evidential value of the document should be left with the court.*

4. *Any party not complying with the requirement to keep a log, or violating other security requirements in relation to the claim in question, should have the burden of proving that the claim is invalid.*

The Computer Code

Preamble

This Computer Code is not intended to be given as an independent statute. The principles of the Code should, however, be implemented in other statutes or regulations, so as to adapt these to EDI technology. Obviously, the propositions set out below have to be based on the traditional regulations. The propositions are to be considered as general rules from which contracts may deviate.

Article 1. Definitions

1. *EDI:* Electronic Data Interchange is the transmission of data structured according to agreed message standards, between information systems, by electronic means.

2. *Message:* A coherent set of data, structured according to agreed message standards, for transmission by electronic means, prepared in a computer-readable format and capable of being automatically and unambiguously processed.

Article 2. Security Aspects

1. Any party transmitting messages electronically should implement measures to avoid transmission errors and alteration of the data.

2. If a message when received appears not to be in good order, correct and complete in form, the recipient should inform the sender thereof as soon as possible.

3. A complete historical record (log) should be maintained of all messages as they were sent and received, without any modification.

4. The log may be computerised, provided that, if so required, the data can be retrieved and stored in readable form.

5. The log should be maintained unaltered and securely, for such time as required by legislation, but for not less than three years.

Article 3. Contract Formation

1. Contracts can validly be concluded and proven by any means.

2. An offer or a response to an offer, made by EDI, becomes effective when it is made available to the information system of the other party.

3. A contract made by EDI, will be considered to be concluded at the time and the place where the message constituting the acceptance of an offer is made available to the information system of the receiver.

   If the message is temporarily stored in, or occasionally passes through, a facility in a third country, the location of the information system interpreting and processing the message should be regarded as the place of contract conclusion.

4. Any party may request the acknowledgement of receipt of the message from the receiver.

5. Acknowledgement of receipt should be given without undue delay, and at the latest within one business day following the day of receipt of the message to be acknowledged.

6. The receiver of such a request is not entitled to act upon the received message, until an acknowledgement has been given.

7. If the message is an offer, the acceptance should also be regarded an acknowledgement, when given without undue delay.

8. When the sender does not receive the acknowledgement of receipt within the time limit, he is entitled to consider the message null and void on so advising the receiver.

Article 4. Accounting and Auditing

1. Vouchers proving the accounting may be based on information which has been transmitted by computerised means.

2. The vouchers may be computerised.

3. The vouchers should be directly printable on paper for one year after the financial year in which registration occurs has expired.

4. Readability of the vouchers should be assured for ten years after the financial year in which registration occurs has expired.

   If the accounting system is being replaced, or for other reasons becomes inaccessible, the vouchers should be printed on paper or transferred to another system or media to secure readability.

5. The vouchers should:
   a) be an accurate and durable reproduction or recording of the messages on which they are based;
   b) be recorded in a systematic manner with no omissions;
   c) be carefully preserved in a systematic way, and protected against any alteration.

6. The log containing the messages on which the vouchers are based should be preserved for a period equal to that of the vouchers.

Article 5. Customs and Excise

1. The information needed for customs declaration purposes could be transmitted by EDI upon permission given by the customs authorities.

2. Whenever a customs declaration or any other information needed by the Customs is being transmitted electronically, the sender is responsible as if the message was signed by him manually.

3. A customs declaration or other information may be sent directly from the exporting country to the Customs of the importing country.

   Whenever a declaration is sent directly from the exporting country to the Customs of the importing country, a copy should be sent to the importer who will be regarded as the declarant.

   The importer should ensure that the content of the message is correct and adequate with regards to what is ordered and expected.

4. Whenever a declaration or other customs information is sent pursuant to no 3 above, the importer should notify the Customs whether the content of the information sent is incorrect or incomplete.

   Such notification should be sent as soon as the importer should be aware of the circumstances causing the notification.

   When such notification is sent, the importer should have the right to alter the information, otherwise he will be held responsible for the content.

5. The customs authorities may withdraw any permission given pursuant to no 1 above if the regulations are not being followed.

6. The information on customs declarations may be stored electronically.

   The requirements for storage of accounting documentation should apply correspondingly.

Article 6. Insurance

1. Transport insurance agreements may be concluded by messages transmitted electronically.

2. The records of such insurance agreements may be stored electronically with the insurer.

3. Any insurance company offering the electronic conclusion of transport insurance agreements, should respond immediately to a message requesting such an insurance.

4. If the insurer fails to respond to such a message, the party requesting the insurance is entitled to consider the request null and void.

Article 7. Evidence

1. Any computer-generated document, message or other such data items received or stored electronically are admissible as evidence.

2. The electronic document must be presented to the court in readable form.

3. Any consideration regarding the evidential value of the document should be left with the court.

4. Any party not complying with the requirement to keep a log, or violating other security requirements in relation to the claim in question, should have the burden of proving that the claim is invalid.

Prior publications in the CompLex series

All reports in the CompLex series may be purchased through the Norwegian Association for Computers and Law, PO Box 7557 Skillebekk, N-0205 OSLO 2. The Association also maintains a subscription service. Subscriptions may be limited to English languages publications, or to «flyers» announcing new reports.

In the list below, English language reports are printed in **bold face.**

CompLex 1/81
Johs Hansen
Et edb-system for analyse av rettslige avgjørelser — *NOK 64,–*

CompLex 2/81
Johs Hansen (red)
Notater om deontiske systemer — *NOK 47,–*

CompLex 3/81
Vidar Sørensen
Informasjonssystem mm for Norges Geotekniske Institutt — *NOK 83,–*

CompLex 4/81
Kjetil Johnsen
Systemtekniske konsekvenser av persondatalovgivningen — *NOK 111,–*

CompLex 5/81
Marit Thorvaldsen
Teledata og rettsinformasjon — *NOK 65,–*

CompLex 6/81
Anne Kirsti Brække
Postmonopolet — *NOK 27,–*

CompLex 7/81
Knut S Selmer (ed)
The LAWDATA Papers — **NOK 28,–**

CompLex 1/82
Norsk forening for jus og edb & Svenska föreningen för adb och juridik
Nordiske personregisterlover,
Council of Europe Convention og OECD Guidelines *NOK 31,50*

CompLex 2/82
Harald Brænd og Vidar Sørensen
Oljevern: Brukerbehov og kildemateriale *NOK 55,–*

CompLex 3/82
Jon Bing og Dag Frøystad
Rettskildebruk *NOK 90,–*

CompLex 4/82
Thomas Prebensen Steen
Post- og televerkets regulerte ansvar *NOK 77,–*

CompLex 5/82
Datatilsynet
Årsmelding 1981 *NOK 44,–*

CompLex 6/82
Birger Eckhoff
in cooperation with Jon Bing, Dag Frøystad and Anja Oskamp
CATTS: Computerized program for teaching text retrieval systems **NOK 61,–**

CompLex 7/82
Jon Bing
Informasjonssystemer for Trygderettens kjennelser *NOK 126,–*

CompLex 8/82
de Mulder, Oskamp, van der Heyden and Gubby
Sentencing by Computer: An Experiment **NOK 123,–**

CompLex 9/82
Colin Tapper
An Experiment in the Use of Citation Vectors in the Area of Legal Data **NOK 56,–**

CompLex 1/83
Arve Føyen
Utredning om endringer i pensjonregisterloven — *NOK 70,–*

CompLex 2/83
Stein Schjølberg
Computers and Penal Legislation — **NOK 140,–**

CompLex 3/83
John S Gulbrandsen og Terje Hoffmann
Rettigheter i idrettsarrangementer — *NOK 64,–*

CompLex 4/83
Sally Moon and Anja Oskamp
The Law of Legal Information Systems: Two Essays — **NOK 95,–**

CompLex 5/83
Datatilsynet
Årsmelding 1982 — *out of print*

CompLex 6/83
Olav Torvund
Betalingsformidling — *NOK 146,–*

CompLex 7/83
Else Ryen
Lov og lovmottaker — *NOK 103,–*

CompLex 8/83
Daniel Stripinis
Probability Theory and Circumsantial Evidence — **NOK 23,–**

CompLex 9/83
Frede Cappelen
Edb-basert informasjonssystem for forvaltningens praksis — *NOK 36,–*

CompLex 10/83
NORDIPRO
Legal Acceptance of international Trade Data — **NOK 142,–**

CompLex 11/83
Jørgen Hafstad og Thomas Prebensen Steen
Teleksrett og merverdiavgift på programvare — *NOK 42,–*

CompLex 12/83
Kristin Kjelland-Mørdre
Om forenkling av regler — *out of print*

CompLex 13/83
Jon Bing
Edb: Mulighet og problem ved forenkling av regelverk — *NOK 92,–*

CompLex 14/83
Tarjei Stensaasen
Utvalgte emner i jus og edb (3. utgave) — *NOK 190,–*

CompLex 15/83
Anette Klafstad og Ulf Alex Samer
Plan for et forsikringsrettslig informasjonssystem — *NOK 60,–*

CompLex 1/84
Jon Erling Skjørshammer
Kabelnett: Bygnings- og ekspropriasjonslov — *NOK 40,–*

CompLex 2/84
Tore Andreas Hauglie og Dag Wiese Schartum
Forslag til et helserettslig informasjonssystem — *NOK 120,–*

CompLex 3/84
Justisdepartementet
Den elektroniske grunnbok — *out of print*

CompLex 4/84
Datatilsynet
Årsmelding 1983 — *out of print*

CompLex 5/84
Tove Fjeldvig
Tekstsøking: Teori, metoder og systemer — *out of print*

CompLex 6/84
Jon Bing
Offentlighetsloven og edb — *NOK 94,–*

CompLex 7/84
Gunnar Bach, Beate Jacobsen and Vidar Stensland
The National Social Insurance System of Norway — **NOK 51,–**

CompLex 8/84
Dag Frøystad
Data Protection in Practice I: Identifying and Matching Elements NOK 80,–

CompLex 9/84
Tove Fjeldvig og Anne Golden
Automatisk rotlemmatisering - et lingvistisk hjelpemiddel for tekstsøking *NOK 90,–*

CompLex 10/84
Elling Øyehaug Ose
Retstidene som informasjonssystem *NOK 120,–*

CompLex 1/85
Jon Bing
Data Protection in Practise II:
International Service Bueraux and Transnational Data Flow NOK 47,–

CompLex 2/85
Jon Bing
Opphavsrett og edb *NOK 176,–*

CompLex 3/85
Dag Wiese Schartum
Codex, Calculation and Computers out of print

CompLex 4/85
Olav Torvund
To informasjonsrettslige arbeider *NOK 52,–*

CompLex 5/85
Datatilsynet
Årsmelding 1984 *out of print*

CompLex 6/85
Hans Chr Aakre (red)
Utvalgte artikler i rettsinformatikk *out of print*

CompLex 7/85
Johannes Hansen
SARA: Brukerveiledning og programdokumentasjon *NOK 150,–*

CompLex 8/85
Johannes Hansen
Modelling Knowledge, Action, Logic and Norms **NOK 90,–**

CompLex 9/85
Thomas Prebensen Steen (red)
Kompendium i informasjonsrett *out of print*

CompLex 10/85
Tarjei Stensaasen
Opphavsrettslovens § 43 («katalogregelen») *NOK 97,–*

CompLex 11/85
Jon Bing
Straffelovens definisjon av «trykt skrift» anvendt på datamaskinbaserte informasjonssystemer *NOK 65,–*

CompLex 12/85
Magnus Stray Vyrje
Vanhjemmel, opphavsrett og datamaskinprogrammer *NOK 161,–*

CompLex 1/86
Anne Kirsti Brække
Formidlingsplikt for kabeleier *NOK 80,–*

CompLex 2/86
Dag Wiese Schartum
Stans av edb-tjenester i krigs- og krisesituasjoner *NOK 80,–*

CompLex 3/86
Ingvild Mestad
«Elektroniske spor» - nye perspektiv på personvernet *NOK 100,–*

CompLex 4/86
Jon Skjørshammer
Opphavsrett, databaser og datamaskinprogrammer: Kontraktrettslige aspekter *NOK 205,–*

CompLex 5/86
Datatilsynet
Årsmelding 1985 *NOK 73,–*

CompLex 6/86
Johannes Hansen
Simulation and automation of legal decisions **NOK 132,–**

CompLex 7/86
Stein Schjølberg
Datakriminalitet og forsikring *NOK 54,–*

CompLex 8/86
Thomas Prebensen Steen (red)
Kompendium i informasjonsrett (2.utg) *NOK 70,–*

CompLex 9/86
Peter Blume
Edb-retlige foredrag *NOK 77,–*

CompLex 1/87
Joseph A Cannataci
Privacy and data protection law:
International Development and Maltese Perspectives **NOK 170,–**

CompLex 2/87
Jon Bing og Jon Bonnevie Høyer
Publisering av rettsavgjørelser *NOK 170,–*

CompLex 3/87
Hagen Kuehn
The Social Security System in the
Federal Republic of Germany **NOK 77,–**

CompLex 4/87
Hanne Plathe Maartmann
Personvern i sykepengerutinen *NOK 70,–*

CompLex 6/87
Jon Bing
Electronic Publishing:
Data Bases and Computer Programs **NOK 55,–**

CompLex 7/87
Ánde Somby
Selektiv gjenfinning av bestemmelser i
bygningslovgivningen *NOK 119,–*

CompLex 8/87
Jon Bing
FOKUS:
Knowledge based systems for public administration **NOK 125,–**

CompLex 9/87
Dag Wiese Schartum
The introduction of computers in the
Norwegian local insurance offices **NOK 230,–**

CompLex 10/87
Knut Kaspersen
Kredittopplysning *NOK 75,–*

CompLex 11/87
Ernst Buchberger, Bo Göranzon and Kristen Nygaard (ed)
Artificial Intelligence:
Perspectives and Implications **NOK 120,–**

CompLex 12/87
Jon Bing, Kristine M Madsen og Kjell Myrland
Strafferettslig vern av materielle goder *NOK 118,–*

CompLex 13/87
Tove Fjeldvig
Effektivisering av tekstsøkesystemer:
Utvikling av språkbaserte metoder *NOK 175,–*

CompLex 14/87
Jon Bing
Journalister, aviser og databaser *NOK 66,–*

CompLex 15/87
Andreas Galtung
Skatterettslig ekspertsystem: Et eksempel basert på
skattelovens § 77 *NOK 82,–*

CompLex 1/88
Robin Thrap-Meyer
Utvalgte emner i rettsinformatikk (4. utgave) *NOK 228,–*

CompLex 2/88
Ernst Buchberger, Bo Göranzon and Kristen Nygaard (ed)
Artificial Intelligence: Perspectives of AI as a social technology **NOK 178,–**

CompLex 3/88
Jon Bing og Anne Kirsti Brække
Satellittfjernsyn *NOK 128,–*

CompLex 4/88
Jon Bing
Journalists, Databases and Newspapers **NOK 68,–**

CompLex 5/88
Joseph Cannataci
Liability and responsibility for expert systems **NOK 108,–**

CompLex 6/88
Datatilsynet
Årsmelding 1987 *NOK 58,–*

CompLex 7/88
Henrik Sinding-Larsen (ed)
Artificial Intelligence and Language
Old questions in a new key **NOK 290,–**

CompLex 8/88
Jon Bing
Database for offentlige publikasjoner (DOP):
Fremtidig organisering
NORIS (87) NOK 178,–

CompLex 9/88
Jon Bing
Conceptual Text Retrieval
NORIS (77) **NOK 118,–**

CompLex 10/88
Henning Herrestad
Alderstrygden i et nøtteskall, eller skall, skal ikke, en studie av anvendelsen av ekspertsystemskall for PC innen det juridiske domene *NOK 108,–*

CompLex 11/88
Ingvild Mestad
L'Informatique, la Liberté Individuelle et la Recherche Epidémiologique
Data Protection and Epideminologic Research **NOK 98,–**

CompLex 12/88
Johs Hansen
SAFE P: Sikring av foretak, edb-anlegg og personverninteresser etter personregisterloven
TERESA (50) NOK 178,–

CompLex 13/88
Henning Herrestad & Dag Syvert Mæsel (red)
Five Articles on Artificial Intelligence and Legal Expert Systems
NORIS (83) FKUS **NOK 108,–**

CompLex 1/89
Dag Wiese Schartum
En rettslig undersøkelse av tre edb-systemer i offentlig forvaltning
NORIS (85) NOK 178,–

CompLex 2/89
Datatilsynet
Årsmelding 1988 NOK 108,–

CompLex 3/89
Dag Syvert Mæsel og Andreas Galtung
XCITE
NORIS(91) NOK 238,–

CompLex 4/89
Robin Thrap-Meyer
Pantsettelse av datamaskinprogrammer og databaser
TERESA(70) NOK 118,–

CompLex 5/89
Ellen-Kathrine Thrap-Meyer
Forbrukerkjøp og EDB
TERESA(58) NOK 178,–

CompLex 6/89
Andreas Galtung
Rettslige aspekter ved
miljøinformasjonssystem
TERESA(72) NOK 118,–

CompLex 1/90
Dag Wiese Shartum
IRIs SPECTRUM
20 artikler i anledning
Institutt for rettsinformatikks
20 års jubileum NOK 298,–

CompLex 2/90
Finn-Erik Vinje (red.)
Språket i lover og annet regelverk NOK 188,–

CompLex 3/90
Datatilsynets årsmelding 1989 NOK 108,–

CompLex 4/90
Eirik Djønne (red.)
Datatilsynet – 10 år som personvernets vokter NOK 108,–

CompLex 5/90
Rolf Riisnæs (red.)
Elektronisk betalingsformidling og forbrukerinteresser I NOK 238,–

CompLex 6/90
Beate Heidenstrøm Hasseltvedt
Rettslige normer og juridiske ekspertsystemer
En vurdering av enkelte sider ved TAXMAN NOK 118,–

CompLex 7/90
Anne Oline Haugen
Offentlig informasjon NOK 148,–

CompLex 8/90
Frank Iversen (red.)
Nordisk rettsinformatikk – Foredrag fra Oslo-konferansen
21. og 22. september 1989 NOK 228,–

CompLex 9/90
Jon Bing
Merverdiavgift og Edb
TERESA (63) NOK 148,–

CompLex 10/90
Jon Bing
Electronic Copying NOK 98,–

CompLex 11/90
Karl Fr. Jarbo
Kabelnett i Oslo-området - Rettslige aspekter NOK 98,–

CompLex 12/90
Henning Berger Herrestad
Norms and Formalization NOK 158,–

CompLex 1/91
Marek Sergot
The Representation of Law in Computer Programs:
A survey and comparison NOK 138,–

CompLex 2/91
Jon Bing
The Portuguese Inforjur Project and Related Issues
NORIS (96) III NOK 128,–

CompLex 3/91
Ola-Kristian Hoff (red.)
20 år med rettsinformatikk – 20 år i forvandlingens tegn
Institutt for rettsinformatikks jubileumsseminar NOK 148,–

CompLex 4/91
Andreas Galtung
Paperless systems and EDI **NOK 198,–**

CompLex 5/91
Rolf Riisnæs (red.)
Elektronisk betalingsformidling og forbrukerinteresser II
Rapport fra den nordiske konferanse 1990 NOK 278,–

CompLex 6/91
Knut Rognlien
Forutberegnelighet og teknologisk utvikling
som juridiske argumenter
NORIS (89) NOK 198,–

CompLex 7/91
Morten Daae
Lovdata – Historie, Lov og forskriftssystem NOK 138,–

CompLex 8/91
Anne Kirsti Brække
Fjernovervåkning og informasjonstjenester
i telenettet
TERESA (83) NOK 238,–

CompLex 1/92
Beate Hasseltvedt
Avskrivninger av mikrodatamaskiner med tilbehør –
en nordisk studie
TERESA (87) NOK 138,–

CompLex 2/92
Nils Kr. Einstadbland
Kringkastingsbegrepet
TERESA (78) NOK 208,–

CompLex 3/92
Maria Strøm
Rettskilderegistre i Helsedirektoratet
NORIS (94) I & II NOK 228,–

CompLex 4/92
Ditlev Schwanenflügel
Softwarepatentet – Imaterialrettens enfant terrible
En redegørelse for patenteringen af softwarelaterede
opfindelser i amerikansk og europæisk ret NOK 158,–

CompLex 5/92
Lars Borchgrevink Grindal
Abonnementskontrakter for kabelfjernsyn
TERESA (78 II) NOK 248,–

COMPLEX

Bestillingskupong

Ja takk, vi bestiller herved følgende eks.
av **COMPLEX:**

.....eks. av nr..... à kr .....

.....eks. av nr..... à kr .....

.....eks. av nr..... à kr .....

.....eks. av nr..... à kr .....

Av fremtidige **COMPLEX** utgivelser (se omtale foregående sider)
bestilles herved:

.....eks. av nr..... à kr .....

.....eks. av nr..... à kr .....

Navn:.....

Firma:.....

Adresse:.....

Postnr./sted:.....

Kupongen sendes til:

Akademika
INTERNASJONAL FAGBOKHANDEL

Karl Johansgt. 47
0162 Oslo 1

This is a different on EDI (Electronic Data Interchange). Although it is based on an analysis of the legal issues raised by EDI, it attemps, unlike other reports on the topic, to suggest solutions for these issues rather than make them subject to further refined analysis.

Jan Freese, Deputy Director General of the Swedish Federation of Industries, currently chairs a Working Party on EDI within the International Chamber of Commerce (ICC). He approached the Norwegian Research Center for Computers and Law with a proposal to develop a report on EDI which was both practical and problem-oriented.

There are presently a number of legal obstacles to the introduction of the new technology and trade represnted by EDI. These obstacles are to be found in the national legislation of many countries. This report identifies typical obstacles, and exemplifies them by reference to national legislation. The report then suggests a remedy to the obstacles in the form of a proposal for regulatory amendments.

TANO

ISBN 82-518-3058-3

9 788251 830584