SPECIAL ON ECMR AND THE ELECTRONIC CONSIGNMENT NOTE

Introduction

The electronic consigment note as an electronic replacement for the paper document has become reality in the world of logistics during the last decade. In 2008 the Additional Protocol To The Convention On The Contract For The International Carriage Of Goods By Road (CMR) Concerning The Electronic Consignment Note, in short e-CMR Protocol, was undersigned by some of the parties to the CMR Treaty.

In 2011 the Protocol entered into force as the minimum of fives States had ratified. Since that date eleven States in total have ratified respectively acceded the Protocol. At this moment (November 2016) the member states are: Bulgaria, Czech Republic, Denmark, Estonia, France, Latvia, Lithuania, Netherlands, Slovakia, Spain and Switzerland.

In the Netherlands the private organisations for shippers resp. carriers developed an internet platform, called TransFollow that is legally compliant with CMR Treaty and eCMR Protocol. This is the first standard electronic consigment note, which can be easily implemented by commercial companies into their enterprise or warehouse or transport software systems. An important feature of this platform is, that it is owned by the independent company TransFollow International, comparable with a third trusted party as mentioned in the article of Professor Maarten Claringbould (paragraph 4).

The articles in this magazine have been published earlier in the Dutch language in Weg en Wagen, nr. 72, March 2014. The articles are now available in English and have been updated by the writers.

The first article of this magazine deals with the literally text of the Protocol, explained by Professor Maarten Claringbould. Other important issues dealt with in this magazine are: Fiscal evidentiary force of the digital consignment note, necessary for VAT-administration; Security of the internet platfom; Protection of data ; Consequences of the use of electronic proof of delivery (POD) that is not compliant to the Protocol. More information on the eCMR Protocol will be published regularly on the website of Stichting Vervoeradres, www.sva.nl. For any more questions or information you can contact the secretary general of this foundation, Mrs. Shula Stibbe (0031-88-5522100 or sstibbe@sva.nl).

Colofon

Publisher
Stichting vervoeradres
Hofweg 33
2631 XD NOOTDORP
Postbus 24023
2490 AA DEN HAAG
T 088 – 552 21 67
I www.sva.nl/wegenwagen

Editor
Mw. Mr. J.S. Stibbe

Lay out
Formzet bv, Zoetermeer

Printing
Formzet bv, Zoetermeer

Electronic consignment note

Explanation of the e-cmr protocol

The text for an additional Protocol to the CMR Convention concerning electronic consignment notes was established in 2008. The basic principle was that the paper CMR consignment note can be replaced by an electronic consignment note which must then contain the same details, in such way that these details cannot be electronically altered. The Protocol only sets out a framework and does not get involved with how things are to be arranged from a software point of view.

Prof. mr. Maarten Claringbould, Professor of maritime law at Leiden University and partner at Van Traa Advocaten

Brief content

The content of the e-Protocol
The e-Protocol consists of 16 articles, but only Articles 1 through 6 are relevant for us. Articles 7 through 16 form the final provisions in which the signing, the ratification, the entry into force (I will come back to this) and the termination and changes of the Protocol are arranged.

1. Definitions

Electronic communication: information generated, sent, received or stored by electronic, optical, digital or similar means in consequence of which the information which has been passed on is accessible for later inspection.

Electronic consignment note: a consignment note issued by the carrier, shipper or another party involved in the performance of the CMR contract of carriage using electronic communication. Details or annexes attached to the e-consignment note can be 'attached' electronically, thus forming a part of the e-consignment note. The electronic linking of details and annexes can also be issued after the e-consignment note has been issued. All of this means that what is 'written down' in said added details becomes part of the contract of carriage laid down in the consignment note. But instructions which are later added to the e-consignment note cannot, in my opinion, bind the original shipper who was unaware of this addition. The consignee will have to watch out, as it is very easy to electronically attach entire volumes (or 'unpleasant' general conditions of the carrier) to the e-consignment note. The question which is difficult to answer from a legal perspective will then be whether an consignee, who is deemed to join the contract of carriage insofar as obligations therefrom for him are set out in the consignment note, is also bound by all the 'small print', which is electronically added to the e-consignment note. Every time he takes receipt of a shipment, the consignee will have to open and study those annexes. This will not happen in practice. It seems reasonable to me to only deem the consignee to be bound by those details which are visible on the e-consignment note itself, i.e. those instructions (e.g. on payment of freight) which are visible on the first opening screen of the e-consignment note. I also believe that industry conditions such as the AVC 2002 would be binding, provided the reference is on the opening screen.

Electronic signature: details in electronic form which are linked to or are logically connected with other electronic details and which function as a method for determining the authenticity. We can seek direct alignment with the European Electronic Signatures Directive (1999/93) and the Dutch legislation based thereon, Articles 3:15 a-f of the Dutch Civil Code. I will come back to the requirements such an electronic signature must meet in order to be deemed sufficiently reliable when discussing Article 3.

2. Scope and consequence of the e-consignment note

This is the core article of the e-Protocol: The electronically prepared CMR consignment note (provided it satisfies the conditions described in Art. 3 Protocol) is deemed equal to the paper CMR consignment note. An e-consignment note is equal to the paper consignment note and therefore has the same evidentiary force and the same consequences as that paper consignment note.

3. Authentication of the e-consignment note

The e-consignment note will be authenticated by the parties to the contract of carriage (these are the shipper, the carrier and ultimately also the consignee) by means of a reliable electronic signature, which signature must of course be linked to that e-consignment note. A method of electronic signatures is deemed to be reliable, if the electronic signature:

a. is linked to the signatory in a unique manner;
b. offers the option of identifying the signatory;
c. is created by means which fall under the exclusive power of the signatory; and
d. is linked to the details to which it relates in such way that later modification of the details can be traced.

Source: This article originally was published in Weg en Wagen 67, October 2008. The text has been slightly shortened and updated by Stichting Vervoeradres)

The foregoing has been taken over to a great extent from the aforementioned Electronic Signatures Directive.

Re a. Uniquely linked to the signatory
There are different ways to 'uniquely' link an e-signature to the signatory: a pin code (credit card system), iris scanning/ handprint, digital signature (written signature is converted into bits and is 'recognised' by the computer the next time) and of course the qualified signature whereby the key lies with a 'Third Trusted Party' (TTP). All relatively costly systems!

Re b. Identification of the signatory
See my remarks under a.

Re c. Exclusive power of the signatory
Strictly speaking, the signature which the shipper and the consignee put on the hand computer used by the carrier is no longer permitted. After all, the hand computer and the software it holds fall under the power of the carrier and not under the power of the signatory. This 'formal' requirement need not be the end of the use of hand computers which run software which cannot (easily) be 'tampered with'. Let's face it, how often does it occur now that a driver delivers the shipment to himself and puts a forged signature of the consignee on the consignment note as proof that he has indeed delivered the goods to the consignee?

Re d. Traceability of later changes
This is a more difficult point if the carrier works with hand computers, on which the driver can simply set out on the e-consignment note during the transport, that upon receipt three items were missing. The carrier must then be able to convincingly prove that the software is programmed in such way that every 'notation' on the e-consignment note will be provided with a time and that it is not possible to tamper with the time specifications. The only way to gain any real certainty about this is if the e-consignment note, the 'notations' and the times are directly transmitted to a TTP or if necessary the shipper. Technically all less easy than it appears to be.

Lastly, Art. 3(3) of the Protocol sets out that the details encompassed in the e-consignment note must be accessible to every party entitled thereto.

4. E-consignment note equal to paper consignment note

It is laid down in Article 4 Protocol that the e-consignment note must contain the same details as the paper consignment note (name and address of shipper, consignee, carrier, goods description, etc., see Art. 6 CMR) and that said details can also be supplemented or altered in the same way as with paper (think of the substantiated reservation of Art. 8 CMR, in which the carrier can state that he cannot count the number of packages, e.g. in the case of closed containers). The software of the e-consignment note must be such that it is established that it cannot be tampered with ("The integrity of details is established if they have remained complete and unaltered"). See also my remarks with Art. 3 Protocol.

5. Implementation of the e-consignment note

Parties to the contract of carriage must agree with each other in advance what procedure and method they are going to use for the e-consignment note. They must also make agreements on the evidentiary force and the like of the e-consignment note. The second paragraph of Art. 5 Protocol states very matter-of-factly that said procedures must be set out in the e-consignment note and that they must be easy to determine.

6. Supplementary documents with the e-consignment note

You would think that with this e-Protocol and the e-consignment note permitted under it, paper would disappear. Nothing is farther from the truth! Paragraph 1 of Art. 6 Protocol reads: "The carrier shall hand over to the shipper, at the latter's request, a receipt for the goods and all information necessary for identifying the shipment and for access to the electronic consignment note to which this Protocol refers". In short, a shipper (but apparently not the consignee) can still ask for a piece of paper with the signature of the driver. I cannot really understand this, as precisely the shipper and the carrier will agree in advance that they are going to work with e-consignment notes and it cannot be the case that the carrier still has to draw up and sign a paper, in which he states that he has taken receipt of the goods for transport. Then you may as well keep working with the current paper consignment notes with carbon copy forms for shipper, carrier, consignee and extra copies.

Paragraph 2 of Art. 6 stipulates that the list of documents which has been added to the consignment note (Art. 6(2)(g) CMR) and the customers documents (Art. 11 CMR) can also be linked to the e-consignment note in electronic form. Those other e-documents must then meet the same integrity requirements as the e-consignment note. See also my critical comments with Art. 1 about the definition of the e-consignment note.

Electronic consignment note

Electronic consignment note in the Netherlands and under the CMR

The use of a consignment note is mandatory in the event of the transport of goods by road. Since 1994 the use of an electronic version of the consignment note in the Netherlands is permitted. Twenty years later, what is the situation with the electronic consignment note in road transport?

Mr. Jos K.M. van der Meché, lawyer at AKD Lawyers and Notaries

1. Introduction

In the past ten years Stichting vervoeradres has regularly paid attention to the electronic consignment note. Examples of this can be found in various publications of the SVA, such as the brochure *'De vrachtbrief'*, in articles in *Weg en Wagen* and in the syllabi of the SVA conference. The transport world is more and more digitalised and the developments in the area of ICT are often innovative. Common examples of successful innovations are the 'tracking and tracing' system and EDI.

In 2016 it is naturally more than common that the agreements between the shipper and the carrier are made electronically. What is easier than quickly sending and replying to an email? Add to this the smartphone. Ten years ago we could barely have suspected that in 2016 the smartphone would bring about such a substantial change in the method of communication and the exchange of data. The electronic consignment note has brought the paper flow virtually to a standstill. Efficient, quick and cheaper.

With regard to the road transport sector it is often said that it is traditional. In my estimation things are not that bad, but in, for example, the air freight sector the use of electronic air consignment notes is far more established. I refer to the use of electronic air consignment notes (e-tickets) in the transport of goods by air. In this contribution the state of affairs is reviewed with regard to the use of the electronic consignment note in the Netherlands and in CMR transport.

2. Domestic road transport

First a word about the legal basis. The use of the consignment note in the commercial transport of goods in the Netherlands is mandated by law. The Dutch Transport of Goods by Road Act and the Dutch Transport of Goods by Road Regulations are crystal-clear on the matter. The Transport of Goods by Road Act stipulates:[1]

'It is prohibited to carry out commercial transport activities if no consignment note has been prepared with regard to said transport'.

The Transport of Goods by Road Regulations flesh this out further and stipulate that the permit holder (i.e. the carrier) must see to it that the consignment note is presented in the delivery truck with which the goods are transported.[2]

But: in the Netherlands a carrier is not obliged to have a paper consignment note on board. If the consignment note details relating to the transport 'are exchanged in a structured and standardised way via an electronic system', the paper version of the consignment note on board of the vehicle is not required.[3] In other words: the exchange of consignment note details via the computer is explicitly permitted, provided that exchange of details has been provided with the necessary safeguards.

The law does not say when there is the structured and standardised exchange of the consignment note details via an electronic system.

This gives the electronic consignment note its statutory basis. The electronic consignment note is therefore a valid transport document.

3. Form of electronic consignment note

We are quick to speak of 'the consignment note', while in practice there are of course various consignment notes for the transport of various goods. Think, for example, of the consignment note for the transport of hazardous substances. In this contribution I have only referred to the commonly known Dutch AVC and CMR/AVC consignment note.

1 *Article 2.13(1) Transport of Goods by Road Act*
2 *Article 15(2)(a) Transport of Goods by Road Regulations*
3 *Article 15(3) Transport of Goods by Road Regulations*

The law does not prescribe any form for the consignment note. The consignment note is form-free. Nor is the consignment note a prerequisite for validly establishing a contract of carriage. If the shipper gives a transport instruction to the carrier, who accepts this instruction, the transport agreement will be a fact. Verbal agreements are also binding! No consignment note is required for that.

The Transport of Goods by Road Regulations do indicate what must be included in the consignment note:[4]

a. the name and address of the shipper;
b. the name and address of the carrier;
c. the name and address of the consignee;
d. the common indication of the nature of the goods;
e. the gross weight or the quantity of the goods specified in some other way.

The road transport legislation only stipulates that both the shipper and the carrier can generate a consignment note. They can also demand that said consignment note is signed.[5] Article 5 AVC (Dutch General Transport Conditions) 2002 stipulates that the shipper must generate the consignment note.

The text of the statute appears to be intended for a paper consignment note, but the statute also says that the signature may be replaced by 'another feature of origin'. This is a step in the direction of the electronic consignment note.

4. Evidence provided by the electronic consignment note

The consignment note has several functions. For example, the consignment note contains the relevant information about the goods on board of the delivery truck and offers the enforcement agencies a tool for inspection. But the most important function is in my opinion the evidentiary force of the consignment note. This can relate to evidence of the contents of the transport agreement, proof of receipt of the goods set out in the consignment note, proof of the conditions of the goods when they have been received by the carrier or upon delivery at the unloading address.

If the electronic consignment note must have that evidentiary function, the consignment note can be deemed an electronic deed. According to the law, a deed is a signed document intended to serve as evidence.[6] With an electronic deed there is no document, but this has been dealt with. Since 1 July 2010, electronic deeds have been legally permitted.[7]

The law does set specific requirements in this respect. Thus the party that wishes to use the electronic consignment note as evidence, must be able to store the contents of said consignment note, in order to be able to use and reproduce those contents later.

Just the possibility of an electronic consignment note is not the end of the matter. The consignment note will also have to be signed. What does the law say about this? When the matter comes to signing an electronic consignment note (i.e. a deed), the law requires an electronic signature.[8]

An electronic signature consists of electronic data which is attached to other electronic data and which is used as a tool for authentification.[9]

This signature is no less than a handwritten signature, provided the method which is used for authentification[10] is sufficiently reliable. The law presents a list of requirements and if this has been satisfied, the reliability will be assumed. An example of such a requirement is that the signature is connected to the signatory in a unique manner.

5. e-CMR

Since the entry into force of the e-protocol with the CMR Convention, with the international transport by road there is also the possibility of using an electronic consignment note.[11] This protocol dates from 2008, but it lasted until June 2011 before it entered into force.
An electronic consignment note is defined in the protocol as a consignment note with the help of digital communication issued by the carrier, the shipper or another party involved in the CMR transport agreement.[12] Data which is logically associated with digital communication (such as annexes) can be linked to the electronic CMR consignment note.

4 Article 15(1) Transport of Goods by Road Regulations
5 Article 8:1119 Dutch Civil Code
6 Article 156 Dutch Code of Civil Procedure
7 Article 156a Dutch Code of Civil Procedure
8 Article 3:15a Dutch Civil Code
9 Article 3:15a(4) Dutch Civil Code
10 The text of the statute says 'authentification', a translation which appears to be derived from the French word authentification. I should think the correct translation is 'authentication'. See also the Dikke van Dale, the authoritative dictionary of the Dutch language.
11 Additional Protocol to the CMR Convention concerning the electronic Consignment Note dated 20 February 2008.
12 Article 1 Additional protocol to the CMR Convention concerning the electronic Consignment Note.

The protocol also provides a definition of the electronic signature. This is data in electronic form which is linked to or is logically connected to other electronic data and functions as a method to determine authenticity.

These signatures are, of course, essential. The e-protocol prescribes that the electronic consignment note must be authenticated by the parties to the contract by means of a reliable electronic signature, which safeguards the link to the electronic consignment note. The e-protocol then indicates when a method of an electronic signature is deemed to be reliable. This is the case, for example, if the electronic signature is linked in a unique way to the signatory and the signing offers the possibility of identifying the signatory.

What is ultimately at issue is that the electronic consignment note has the same status as the paper version of the consignment note. The e-protocol determines that as well. A digital consignment note which satisfies the provisions of the e-protocol, is deemed equivalent to the paper version and has the same evidentiary force and the same consequences.

The electronic CMR consignment note must contain the same details as the paper consignment note. Article 6 CMR Convention provides a list of details which the consignment note must contain. It must be possible to supplement the details in the electronic consignment note with, e.g., the reservation of the carrier.

All in all the e-protocol offers the parties to the contract of carriage the option of agreeing that an electronic consignment note is used. The e-protocol has entered into force and in the meantime eight countries have ratified the e-protocol or have joined the protocol. This are: the Netherlands, Bulgaria, Estonia, France, Spain, Latvia, Lithuania, Slovakia, Switzerland, the Czech Republic and Denmark.

6. A brief look at practice

The list of countries mentioned above directly indicates that in practice it is still difficult to use only an electronic consignment note. After all, if the national legislation of a country that the driver crosses prescribes that a paper version of the consignment note must be on board of the vehicle, the parties to the contract of carriage do not benefit that much from an electronic consignment note. For example, Belgian law stipulates that the driver must be able to present a paper consignment note to the enforcement agencies in the event of an inspection in Belgium.

Belgium signed the e-protocol on 27 May 2008, but has not ratified it to this day.

Many routes can be conceived where the driver will encounter the same statutory provisions. There is a favourable exception: transport of goods from Latvia to Lithuania (neighbouring countries) and back can be carried out in its entirety with an electronic consignment note. However, as I understand it, the cooperating business organisations in Stichting Vervoeradres (EVO, NBB and TLN) are lobbying in Brussels to have the E-protocol apply throughout all of Europe.

7. Conclusion

It is high time to fully utilise the options which Dutch legislation and the e-protocol offers when it comes to the electronic consignment note. Efficiency and cost savings are key terms in the transport industry. There are impediments in the form of rules in many European countries, which still make paper mandatory.

Beurtvaartadres is making great strides with TransFollow, with which shippers, logistics service providers and consignees can enter, exchange and sign a consignment note with one uniform and standardised interface. This secured, standardised digital solution offers the sector a chance to optimise the current consignment note processes and to improve the communication in the chain. In the event of successful implementation of that new standard in the Netherlands lobbying in Europe will be easy and that standard will be able to spread across Europe.

Electronic consignment note

Fiscal evidentiary force of the digital consignment note

For application of the VAT zero rate for exports, or for intracommunity supplies it is required, inter alia, that the party who supplies the goods, can demonstrate that the goods have actually left the Netherlands. A commonly heard question is how that transport must be demonstrated to the Revenue Service. Is the electronic consignment note sufficient for this?

Mr. Roelof Andringa, partner at Andringa Caljé & De Jager lawyers

1. Introduction

As always, actual practice needs clear guidelines regarding which documents must be present in the administration to be able to demonstrate the transport to a foreign consignee, e.g., in the form of a list of minimum requirements. But there is no real fixed list of minimum requirements.

The law only says that the zero rate must be demonstrated by books and documents. The transport can thus be demonstrated by all possible means, provided those means are in writing. The possibility of being allowed to use all evidentiary means is known as the "flexible evidence doctrine". On the opposite side of the flexible evidence doctrine is the situation that the law explicitly prescribes what evidentiary means are required or permitted to constitute proof.

2. What is the flexible evidence doctrine

As stated, the flexible evidence doctrine means that all forms of evidence are permitted. The flexible evidence doctrine also means that the court is free to assess the evidence presented by a tax subject. In the assessment of the evidence the court will take account of the reliability of the details in said evidence, and this raises the question whether and if when electronic data is reliable.

No general rules have been given for this, and thus the court will assess the reliability of electronic data on the basis of the context in which the data is found, as well as whether the data is contradictory, or otherwise shows defects, and to what extent integrity (contents) and authenticity (shipper) is safeguarded. The fact-finding court is free to use only that evidence of all the available evidentiary material, which seems useful from the perspective of reliability, and to set aside what the court deems of insufficient value to constitute proof. In principle the court does not have to give reasons for that decision.

Evidence can in any event not be dismissed just because the matter concerns electronic data. On the contrary, today electronic data forms an increasingly important part of our society and the government is adapting to this, for example by explicitly approving that data may be furnished or stored in electronic form. That general acceptance of electronic data appears, for example, form the Decision of the Revenue Service on Administrative and Invoicing Requirements, in which it is explicitly stipulated that the invoice is one of the most important documents to be able to determine the input tax and the VAT to be paid, and that the invoices may not only be presented in writing but also electronically because the basic principle is that paper invoices and electronic invoices must be treated the same. The only condition is that the customer implicitly or explicitly accepts the electronic transmission, and that the shipper of the invoice has guaranteed the authenticity of the origin, the integrity of the contents and the legibility of the invoice. I only wish to demonstrate with this that the Revenue Service already allows important documents, such as the invoice, to only be available electronically.

3. Electronic consignment note

The electronic consignment note can thus be used as evidence in fiscal matters and I expect that the courts will also deem it an important evidentiary tool because a lot of attention is paid to safeguarding the integrity of the contents, and the authenticity of the origin of the electronic consignment note, not in the last place because the supplier will always have access to an electronic consignment note signed for receipt, while the suppliers who make use of paper consignment notes, often only have the send copy.

I know that in the discussions on options to prevent VAT fraud, attention has been paid to a system whereby a supplier can only claim application of the VAT zero rate at the time that the supplier receives a confirmation of receipt. In essence that is what the German *Gelängenbestätigung* does. When the electronic consignment note does become the standard in European logistics, it would not surprise me if the Revenue Service deems the 'clearance' of the electronic consignment note, in the mid-long term, as a prerequisite for applying the VAT zero rate.

4. Note, the electronic consignment note is not sufficient

Lastly, I would like to stress that the current jurisprudence shows that a (copy of a) consignment note alone is not sufficient evidence for the application of the VAT zero rate. In the judgment of the Netherlands Supreme Court of 18 April 2003, no. 37.790 the Supreme Court held that the applicability of the zero rate must appear from books and documents, and that the submission of copies of the invoices, CMR consignment notes, packing notes, payment receipts, and statements of the transport company, collectively form sufficient evidence, provided said evidence does not have any defects.

The (electronic) consignment note is thus a very important evidentiary tool, but according to the current state of jurisprudence increasingly more evidentiary means are necessary than just the (electronic) consignment note.

Electronic consignment note

A question from day to day practice:

Is it wise to sign for receipt on a screen?

Question:

Courier services, package services and distribution transport often use the on-board computer or the driver's mobile phone to create proof of receipt. The consignee signs on the screen that the driver presents to him, indicating to have received the shipment in good condition.
The advantages of this system for the carrier are easy to summarise: no more paper consignment notes and the digital proof of receipt can quickly be passed on to the carrier's head office. The principal (the shipper) can follow the shipment on the carrier's website using a login code and can review the proof of receipt, so that he knows that the goods have arrived at the consignee's.

But what is the legal value of such a signature for receipt? Is it a safe method for all parties?

Mrs J. Shula Stibbe, secretary general of Stichting Vervoeradres

Answer:

Consignment note

One of the functions of the consignment note is that it is a record of the contract of carriage. All parties involved in the contract of carriage will receive the same copy of the consignment note. With an electronic consignment note on the on-board computer, the consignment note will only be available in the carrier's on-board computer. Neither the shipper nor the consignee will have access to the same copy. Even if the carrier sends a digital copy to the other party (shipper/consignee), there is no independent party to guarantee that the digital copies have not been altered. The consignment note serves as proof of the agreements made in the contract of carriage. If these agreements are recorded in this digital form, the evidentiary proof of such electronic or digital consignment note is dubious.

Signature

Dutch legislation makes an electronic signature possible, and the parties may agree among themselves to what extent the electronic signature they use must be unique and secured. Should one of the parties dispute the validity of the signature, the court will determine whether the (technical) method which was used for the electronic signature, makes the signature sufficiently reliable "in view of the goal for which the electronic data was used in view of all other circumstances of the case". The closer the technical quality of the electronic signature is to the reliability requirements laid down in the law, the greater the reliability and concomitantly the evidentiary force.
The parties can opt for a qualified signature, as this is irrefutable. Such an electronic signature is based on a qualified certificate, which is issued by a certification service provider and which satisfies all statutory requirements. Unfortunately such a qualified signature is expensive and inflexible, because both parties have to use the same software system.
The signature on a screen ("sign on glass") is not very reliable and therefore has limited evidentiary force. The software used is in the hands of the carrier, and therefore cannot be checked by the shipper/consignor. The signatory will not immediately receive a copy or a 100% reliable copy of the signed confirmation of receipt, as is generally the case with a paper proof of receipt. Nor is it possible for the consignee to determine whether his signature, which he put on the screen, is connected to the electronic file of the consignment note. Because the technology is in the hands of the carrier, he could separate the signature, change details afterwards and even use the signature for other purposes.

Proof of receipt, copy with recipient

The proof of receipt constitutes evidence that the carrier has concluded his transport assignment. The period in which the carrier was liable for the goods transferred to him, is hereby concluded. After issuing the clean proof of receipt the consignee can only claim loss from the carrier in exceptional cases. A claim for loss on the part of the seller under the purchase contract will be more difficult to substantiate.
After signing for receipt on a screen linked to a system of the carrier, the consignee will not receive a copy or not a 100% reliable copy of the proof of receipt created in this way. Nor are all details about the goods and the transport always visible on the screen and it is often unclear how and/or whether remarks and comments can be noted. The consignee signs more or less blindly and will not receive a (reliable) copy. From a practical and commercial perspective the working method is understandable: signing on a device is cheap, fast and efficient. Legally, however, this construction is not recommended.

Security

The reliability of electronic signatures can vary significantly, depending on the degree:

- in which a signature is secured (secured by encrypting or unique codes) and
- is linked in a secured manner to the document for which the recipient signed and
- is stored in a way that the details cannot be unilaterally changed after acquisition

How the signature on a screen ("sign on glass") is secured, depends on the choices which the carrier has made. In general that cannot be seen on the screen.

The TransFollow electronic consignment note is safe and innovative

Consignment notes in on-board computers or website portals have in common that the carrier is the owner of the system. It is better to generate the consignment notes via TransFollow. This independent platform has been developed on instruction of the representatives of the logistics chain in the Netherlands (EVO/TLN/NBB). This platform, called TransFollow, is independent in such sense that parties to the contract of carriage have no control over the standards and security of TransFollow. Once a party has generated a consignment note, all later changes are visible for the other parties to the contract of carriage. By working with a platform it is not necessary for the parties to use the same software. In addition, the TransFollow security is certified and signatures are unique due to the use of one-off QR codes. The evidentiary force of the TransFollow consignment note is consequently the same as the paper consignment note.

Electronic consignment note

Electronic consignment notes via the TransFollow platform: a new cloud service

Providers of cloud services, like TransFollow, must comply with the Dutch Personal Data Protection Act and see to technical and legal continuity. What must you look out for if you make use of a cloud service?

Matthijs van Bergen
legal adviser and security officer at ICTRecht

1. The advantages of an electronic consignment note

In the transport world things are progressing in the area of ICT. As in essence is the case in every sector, important efficiency advantages can be achieved by the smart use of ICT. An example of this is the system for electronic consignment notes, which is currently being developed by Beurtvaartadres, TLN and EVO, called TransFollow.

Consignment notes are of vital importance for the transport world. An important function of the consignment note is the proof of agreements between shipper, carrier and recipient, as well as the proof of the time and the place of transfer of the goods (taking into receipt by the carrier, delivery to the consignee). In everyday practice working with all kinds of (carbon copy) sheets of paper completed by pen and signed is less handy and efficient than an electronic system that runs in the cloud. Indeed, it is said that the Netherlands logistics sector could save approx. 675 million euros a year with the electronic consignment note. Such savings could be possible thanks to TransFollow, because via TransFollow a pre-notification can be made to the shipper/unloader or recipient with details regarding pick-up and delivery. In this manner waiting times can be limited and delivery discrepancies can be prevented.

2. Cloud services

Everyone who knows Gmail, Dropbox, Facebook, Twitter, WhatsApp, LinkedIn, Instagram, WeTransfer and similar services, and these days that is almost everyone, knows how handy and time-saving cloud services and apps can be.

From the perspective of the commercial customer and user, cloud services have other important advantages in addition to the ease of use for the user. Because in essence a service is being outsourced and hired, (the ICT department of) the customer/user does not, for example, have to acquire hardware and software itself to develop and supply the service. The hardware and software with which the service is offered, runs in specially set up and professionally run datacentres, while a simple laptop, tablet or smartphone with internet connection and a standard browser suffices to be able to make use of it. Another advantage is that cloud services can usually be scaled very flexibly. If more is necessary, whether this is in terms of computing power, storage, user accounts or functionalities, this can often immediately be delivered on demand.

The most important disadvantages for customers lie in the fact that they relinquish control over the availability and the security of the services and the data processed therein. That is why many companies are still wary of the idea of becoming dependent on cloud-based services. Because successful providers serve an enormous number of customers at the same time, they have a wealth of valuable and sensitive data under their control. Certainly in a time of long-term financial malaise and a substantial increase in criminal hacks and data leaks, it must be no doubt that the service and the data processed with that service are continually available and properly secured against loss, harm and illegal access. Before companies switch from more traditional ICT to apps and cloud services, they must also properly ascertain the safety and reliability thereof. For companies which offer or procure cloud services, a number of measures are obliged by law and a number of additional measures are recommended from a legal perspective.

3. Compulsory measures

If personal data are (also) processed in the cloud service, which is almost always the case these days, it is obliged by law to make a *data processing agreement*. In said agreement the provider and the customer legally arrange how the privacy of the data subject is protected and what technical and organisational measures are taken to secure personal data against loss and illegitimate processing.[1]

Data processing agreements are of great importance for safety and continuity with cloud services. Often there is a long chain of service providers who work together to be able

[1] *See Article 14 Dutch Data Protection Act.*

to provide the cloud service. One company programs the software, while another company exploits and sells it, via external distributors or otherwise. The hosting (running and making available via the internet) of the software is often purchased from an external hosting provider, who in turn may hire rackspace (room on which to hang physical servers) in a datacentre. All these parties often have de facto access to the data of the cloud service.[2] In data processing agreements, all links in the chain make agreements between themselves about how the safety and continuity of the cloud service is safeguarded.

Normally a clear *privacy policy* must have been published in which information is offered for the relevant parties regarding the purposes for which personal data is processed, how data subjects can gain insight into their personal data and how this data is processed and it what manner they can ask for corrections. The privacy policy can also give some general explanation to the data subjects regarding the level of safety that they can expect.[3]

4. Recommended measures

Hacks, cyber crime and data leaks are important topics these days, which also make the daily news. More and more companies realise the risk that they might be the next one to make the front page. In addition, the Dutch Data Protection Act compels companies to take suitable security measures against loss and illegitimate processing of personal data. Although the law does not mandate the following measures in so many words, they are recommended to comply with the duty to protect data.

4.1 Security protocol

For example, it is recommended to draw up an information security protocol for internal use. The protocol enables everyone in the organisation to deal with personal data in a safe and 'hygienic' manner. A security protocol can also be included as an annex to the mandatory processing agreement.

4.2 Incident scenario

Because no single measure can guarantee for 100 percent that no incident will ever take place, it is also wise to draw up an incident scenario. If a group of hackers should have run off with a database full of personal data, a previously prepared scenario can help the organisation to take the right actions quickly and to avoid making the damage worse by panicking.

4.3 BYOD regulations

Because these days employees sometimes also use their own devices for their work, *bring-your-own-device* regulations are a good idea. This can limit the risk that a laptop or smartphone of an employee is the weak link in the security chain, with which unauthorised parties can gain access to sensitive databases.

4.4 Ethical hacking? Responsible disclosure policy

A responsible disclosure policy helps to ensure that the activities of ethical hackers work out positively for the organisation, instead of negatively. A good responsible disclosure policy clearly indicates what ethical hackers must comply with and how they might be rewarded if they make a contribution to increasing security by properly following the rules.

4.5 Implementing a standard, like the ISO 27001 and 27002 standards

The Dutch Data Protection Authority refers in its guidelines 'secured personal data' to various standards and best practices to come to good information security. With the help of ISO 27001 an organisation can, for example, set up an 'information security management system' (ISMS), while ISO 27002 primarily contains examples of concrete security measures which can be implemented.

4.6 Taking out insurance

These days more and more insurers also offer special insurance for hacks, data leaks and privacy problems. In addition to the above measures, insurance can help to limit the risks. The exclusions and limitations must be taken into account, as must the excess and other hidden costs.

5. Safeguarding continuity

If the provider of the cloud services goes bankrupt, all its customers have a big problem. Normally speaking they no longer have access to the service on which they are now dependent and where they stored a lot of important data. There are legal solutions to safeguard that the business activities of customers of cloud services do not come to a standstill if the provider goes bankrupt. In essence these solutions focus on the essential components of the service being placed as much as possible in separate legal entities (trusted third parties, TTPs) which are not dependent on the solvency of the service provider and bear as little (business) risk as possible. For example, this could be a foundation which has the goal of safeguarding the continuation of the service...

[2] *Not to mention all providers of internet access and transit, over whose networks the data are actually transmitted.*
[3] *Article 7 Dutch Data Protection Act stipulates that personal data is only gathered for specific, explicitly described and legitimate purposes. Articles 35 and 36 regulate the rights of inspection and correction for data subjects.*

6. Consignment note in the cloud with safeguards

As has been explained above, there are risks connected with the use of cloud services. In order to convince loaders and carriers of the possibilities of consignment notes in the cloud, safeguards about that 'cloud' will have to be transparent. For the success of the electronic consignment note it is crucial that the availability, integrity and confidentiality of the consignment notes and other information stored in the system is conscientiously managed and guaranteed by the provider.

Electronic consignment note

Smart Transport?

About consignment note Apps, electronic signatures and trust services

The validity of electronic signatures and contracts is based on EU legislation. The former Directive 1999/93 EC was replaced in 2014 by Regulation 910/2014 EU which has direct effect. What does this mean for the electronic consignment note?

Prof. Dr. Arno R. Lodder is Professor of Internet Law at the Vrije Universiteit in Amsterdam

1. Introduction

Peculiarly, as a guest writer of *Weg en Wagen* I do not have a lot of affinity with the regular columns: waste transport and customs law. Although I did work in rubbish collection for a few weeks in the 1980s. This is my only link to the columns in *Weg & Wagen*, which, as an internet lawyer, I do not know much about. There are parallels between transport and the internet. Particularly in the early days the "electronic superhighway" was used as a metaphor for the internet. Last year Neelie Kroes spoke of thresholds on the superhighway, when the matter concerned legislative bills relating to filtering and blocking by Internet Providers.

Where the two infrastructures particularly come together is in electronic commerce: goods ordered over the internet must in the end be transported from the seller to the buyer. After a Chinese film on YouTube in 2013 where pastries were delivered to people's homes by a drone, large suppliers like Amazon started thinking of delivery by drones. The complexity of a small, flying drone autonomously finding its way through the air based on geo-information is less complex than the driverless cars that have been driving around for a number of years. At least, cars which are not operated by the driver. It is of course possible that things will become just as congested in the air as on the road and consequently complexity increases, but things have not got that far yet. Will it be possible to increase the scale so that drones can also carry large shipments? I don't think so, but then I would not have thought that a 3D printer would be able to print real houses, so who knows. For the time being a lot of freight transport is still by road.

Just as in every industry branch, information technology has been playing a role for a long time. The internet has been in use for almost as long, and in the last few years smart mobile devices like smart phones and tablets have also come into play. In this contribution I will go into the use of electronic communication in commercial traffic. My focus will be on describing the Rules relating to electronic signatures, which is also the title of a book that I wrote together with Jos Dumortier and Stephanie Bol in 2004/5. The rules from the Dutch Civil Code relating to electronic signatures will disappear soon. Instead, a European regulation will regulate not only signatures but also topics of interest to the transport sector such as electronic seals and electronic time stamps.

2. Consignment notes: from on-the-road printing to Apps

A formal analysis of incoterms for electronic commerce by Tan, Mitrakas & Thoen (1998) describes a supporting system, INCAS, that automatically reasoned with the Incoterms® (International Commercial Terms), the delivery terms and conditions drawn up by the ICC (International Chamber of Commerce). Everyday practice has not yet reached this point. Use is being made of electronic consignment notes which can then be printed on the road. The company PrintCMR offers the option of printing consignment notes "in the cabin or simply at the office". The next step is to completely eliminate the paper link. The Innectis App for consignment notes is paperless:

> *"The user will see a summary of all available consignment notes on his account. This can be divided in various ways, e.g. on the basis of a route, date, geographic spread. A specific consignment note can be quickly tracked down by means of a search function."*

The App uses geo-locations and time stamps, so that it can be reviewed later whether a relevant shipment has been delivered or picked up. Various levels are used for the signing, i.e. "with pen, via login, with a token, via a QR-code".

Everyday practice is clearly ready for electronic consignment notes – is the law?

3. Electronic signatures

In May 1995 the first legislation relating to electronic signatures was established, the Utah Digital Signature Act. This was followed in Europe in 1997 by Italy *(Legge Bassannini)* and Germany *(Signaturgesetz)*. To prevent a range of different regulations in member states, Directive 1999/93/EC on Electronic Signatures was adopted in the European Community. In May 2003 the section *"1a. Electronic legal transactions relating to property rights"* was introduced into Book 3 of the Dutch Civil Code (DCC). Art. 3:15a DCC is the key provision, stipulating that an electronic signature is in principle the same as a written signature. The conditions for validity are broadly formulated: the method used for authentication must be sufficiently reliable. In order to determine this the purpose for which the electronic data is used must be reviewed, as well as all other circumstances of the case. Van der Meché discusses what this means for electronic consignment notes in this issue in the article *"The electronic consignment note in the Netherlands and under the CMR"*.

From a legal perspective there is thus no impediment to, e.g., signing consignment notes electronically. That Section 1a of the Dutch Civil Code will be amended soon does not change this. To replace and expand on Directive 1999/93 EC, the European Union adopted Regulation 910/2014 EU on electronic identification and trust services for electronic transactions in the internal market in the spring of 2014.

4. Regulation of electronic trust services

Whereas member states must convert a directive into national law, a regulation has direct effect in the national legal system of the EU member states. Regulation 910/2014 EU has two advantages. In the first place, it is based on the Services Directive 2006/123/EC. Pursuant to said directive, companies and citizens of member states must be able to obtain information in every member state in their own language regarding rules relating to business activities intended in another member state. The currently proposed regulation obliges member states to furnish every citizen and every company with an electronic identification tool accepted within the EU. A kind of advanced, international DigiD. The second part of the Regulation is more relevant for road transport and consignment notes:

> *"establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, services for electronic delivery and website authentication."*

Electronic seals - and time stamps in particular - are a novelty and of importance to the transport sector. Although the draft legislation whereby a legal framework is created for electronic recorded mail, electronic archiving and electronic time registration was approved by the Parliamentary Committee for Enterprise in Belgium on 28 October 2013, this legislation will become redundant to a great extent after the entry into force of the proposed Regulation.

4.1 Validity of electronic information

Just like in the Electronic Signatures Directive, the Regulation describes various levels. For example, on the basis of the Directive the user of a qualified signature is certain that it is recognised in all member states and there is a legal presumption that the signature is valid. With qualified signatures use is made of certificates which can only be furnished by special designated service providers. Although the term qualified signature is used commonly in the literature, the term 'qualified' was only used in the Directive to specify the type of certificate as just indicated. In the Regulation, for every trust service an explicit distinction is drawn between a regular and a qualified version. Just as previously with the signature, the latter automatically entails legal consequences.

The regulation of every trust service starts with the stipulation which underlines the self-evident use of electronic information:

> *"The validity of an electronic [...] and the admissibility thereof as evidence in judicial proceedings may not be denied purely on the basis of the fact that [...]is electronic."*

In 1996 it was comprehensible that in Article 9 UNCITRAL Model Law on E-commerce it was stated that the evidentiary value of electronic information could not be denied merely by arguing that the information is electronic. It is surprising that this is still deemed necessary in the year 2014.

4.2 Seals and stamps

An electronic seal is used "to guarantee the origin and integrity to safeguard the data connected therewith."
An electronic consignment note can, for example, be provided with such a stamp. If use is made of a qualified certificate, the following applies (Art. 28 of Regulation 910/2014 EU)):

> *"the legal presumption that it guarantees the origin and integrity of the data to which it is connected."*

An electronic time stamp connects electronic data, for example an electronic consignment note

> *"to a specific time and which prove that said data existed at that time."*

Here too if a qualified time stamp is used, there is the legal presumption "that the specified time and the integrity of the data linked to the time, are guaranteed."

5. Close

Everyday practice is ready for electronic document exchange in the area of road transport. The law has recognised electronic signatures since 2003. In 2014 the electronic seal and time stamp were added to this on the basis of the aforementioned EU regulation. If a qualified version accompanied by safeguards is applied, the carrier is assured of a legal presumption that the data and the time are correct. With less substantial versions than the qualified one the Regulation creates, in addition to the already existing signature (name under email, electronic pen signature), a legal basis for, inter alia, electronic time stamps and seals. It is possible that in time the road carrier will be replaced by unmanned trucks or helicopters. Until that time physical transport by road can in any event be combined with legal safeguards relating to electronic information.

Standardised digital consignment note platform (Stichting vervoeradres)

The road to paperless road transport has turned out to be difficult to realise in practice. At present primarily interim forms are common, such as Apps whereby data is entered via an internet application but is then printed as a consignment note on paper.

There are various sign-on-glass solutions on the market to replace the paper consignment note. Sign-on- glass means that the recipient signs on the screen of the portable device that the driver carries with him. This consignment note and signature entails a lot of problems:

- From a legal perspective the signature is not an original, but a copy;
- The signature is not linked to the consignment note;
- The consignee does not receive a copy of the consignment note;
- The digital information is in the possession of the carrier. It is thus possible that the carrier will make unilateral changes to the digital consignment note and signature.

The platform called TransFollow, solves the above problems. With a standardised interface all ICT and consignment note App suppliers can make a link to the TransFollow platform. The consignment note can then be submitted electronically on the TransFollow platform by means of the company's own TMS or WMS package (via an API link).

In addition, the consignment note is accessible for all chain participants: shipper, forwarding agent, carrier, sub-carrier and consignee.

At the time that the shipper indicates on his App to have transferred the shipment, a unique code (numbers series or QR code) is visible on the App.

By entering this code on the carrier's on-board computer, the carrier agrees to receipt. Upon delivery to the consignee, the consignee in turn receives a unique code on his App to 'sign' for receipt on the carrier's on-board computer. In time the QR code will probably be replaced by NFC (Near Field Communication) so that contactless signing of the digital consignment note will also be possible and the signing process will become easier and more reliable.

Electronic consignment note

Transport companies and privacy

Transport companies possess personal data as service provider and as employer. In both roles they have to deal with privacy legislation. Firstly the company must know its position: processor of personal data or data controller. In this article obligations under the European General Data Protection Regulation are explained.

Koen Versmissen is a partner at Privacy Management Partners[1]

Daphne Methorst-Smaling is a legal adviser with Transport en Logistiek Nederland[2]

1. Introduction

In this contribution we will go into the importance of privacy for transport companies. First of all we answer the question "What is privacy?". We explain what data-driven business is, and that is what the privacy legislation is really about. Then we will discuss the basic principles which are intended to ensure that that data-driven business takes place in a decent manner. After that we have a look at the degree to which transport companies have to deal with privacy rules. Of great importance in this respect is the distinction between two important roles of the transport company: service provider and employer. In short, the service provider generally does not have that much to do with privacy, but the employer does all the more. Lastly, we discuss the legislative change of 1 January 2016 and the European General Data Protection Regulation which will enter into force as of 25 May 2018.

2. What is privacy?

2.1 Personal data-driven business

Strictly speaking, privacy is about screening out private affairs: we prefer to keep some things to ourselves. But when we speak of statutory privacy rules, we really mean: rules for properly and carefully dealing with personal data. Personal data is all data about people: not only their name, address and telephone number, but also information about their health, what they do in their free time, how they function at their work, where they have been and what they have done, you name it. For more and more companies and government organisations, personal data is the driving force behind the most important processes. Privacy rules are thus rules of the game for personal data-driven business. Because transport companies have data-driven business, we will review in paragraph 3 to what extent that means *personal* data-driven business.

2.2 Core obligations

The general statutory privacy rules can be found in the Dutch Personal Data Protection Act. In addition, certain industries still have their own regulations, which often also include privacy rules. As stated, privacy regulations are all the rules about how you must and may deal with personal data. For the transport sector the matter concerns, e.g., rules about consignment notes and the digital tachograph. All those privacy rules are fairly complicated. In the end they come down to the following five core obligations for companies which process personal data (storage, use, etc.):

1. ***Privacy management*** – Whoever processes personal data, must first of all establish the policy therefore; that policy has to be translated into suitable measures which ensure that personal data is dealt with according to the rules, think of instruments such as information, training, procedures, contracts, audits and ICT measures (e.g. against hackers); those measures must be documented and monitored, so that it can be demonstrated that they are effective (guaranteeing a suitable security level and preventing unnecessary processing).
2. ***Balanced solutions*** – What measures have to be taken? The privacy risks can be charted with a "Privacy Impact Assessment" (PIA). The matter concerns the risks of careless or improper processing for both the persons in question and for the organisation which processes the data. The outcomes of a PIA form the starting point for taking management measures. A data controller can*not* reason that such measures are not necessary because the chance is too small that a problem will arise. It is, however, possible to establish priorities as not all privacy problems weigh equally heavily. There is also room for efficiency: Rolls Royce solutions are not necessary if Volkswagen solutions will suffice.
3. ***Appropriate data processing*** – Privacy legislation is primarily legitimating legislation: whoever remains within the statutory framework, may process personal data. The core of those statutory frameworks is: appropriate data processing. For example, there must be a clear and justified purpose for the data processing and the data processing must also be necessary to achieve that goal. Nor may more data be processed than necessary and the data must be sufficiently accurate and up to date. The matter is different for certain sensitive data, the processing thereof

[1] *Koen Versmissen is a partner at Privacy Management Partners (www.pmpartners.nl). Privacy Management Partners offers practical solutions for proper and careful data processing in accordance with the law.*
[2] *Daphne Methorst-Smaling is legal adviser with Transport en Logistiek Nederland (www.tln.nl).*

is "prohibited, unless…".The matter then concerns, for example, data about someone's health, sexual orientation or criminal past.

4. ***Privacy services*** – The person to whom the personal data relates (the data subject) must, subject to statutory exceptions, always be informed prior to the data processing. The privacy legislation gives everyone the right to submit complaints or requests to data controllers. A data controller must in the first place be transparent about the forms of processing and about where someone can go with questions and complaints. Every request of a person for inspection, correction or removal of his or her data must have been dealt with within four weeks. This does not mean to say that a requesting party must get his way in all cases, but in the event of dismissal this will have to be checked and substantiated properly from a legal perspective. If a request must be heeded, then this must naturally be implemented.
5. ***Chain management*** – These days various parties often work together, both internally and externally, or information services are shared. For example, it frequently occurs that an employer has outsourced his payroll administration to a specialised service provider. Instead of one, two parties will then be involved: the customer and his implementation organisation. Thanks to the internet and the creation of cloud services this complexity is only increasing, whereby service providers can be based anywhere in the world. What is particularly relevant in this respect is that the customer retains final responsibility for compliance with the privacy rules. He can thus be held responsible for mistakes made by his service provider. In addition, he is obliged to make a data processing contract with the service provider in which the interests of the data subject are safeguarded.

3. Transport companies and privacy

In this paragraph we will review to what extent transport companies have personal data-driven business, and thus to what extent transport companies have to deal with the privacy rules.

3.1 The transport company as service provider

What does the transport company have to do with the privacy rules in its capacity as service provider? We can answer that question in a number of steps.

The first question is whether personal data is being processed. This is indeed the case. In many cases a transport company receives the name and the address of a person to whom goods are to be delivered. This immediately means the *processing* of personal data, as this is a very broad term: storing data, using data, giving data to other people, destroying data, it's all covered by the term 'processing'. It is this processing we will focus on below.

The second question is whether that processing falls under the Dutch Personal Data Protection Act. This will virtually always be the case. The Personal Data Protection Act applies in any event to every automated processing of personal data by a company. For example, when use is made of electronic consignment notes, of software for the planning of routes or of camera supervision. A paper data collection is also covered by the Personal Data Protection Act as soon as it has been structurally organised. Do be aware that not all data gathering is permitted! A number of specific topics will be further reviewed by the Dutch Data Protection Authority.[1]

The third question is, what is the role of the transport company. In paragraph 2.2 we specified a number of core obligations for the person who processes personal data on his own initiative or instructs another party to do such. This first person is called the *data controller*. The first person who processes personal data on the instruction of a data controller, is called the *processor*. This is an important difference, because the data controller has more obligations and can be held primarily liable for the processing.

If a customer engages a transport company for the transportation of goods, in general the customer will be the data controller (unless he is himself a processor for another party) and the transport company is the processor. The transport company must know from whom the goods must be picked up and to whom the goods must be delivered. Such data processing is primarily intended to serve the shipper and the recipient, not the transport company.

The matter becomes different if the transport company were to process the data for itself, e.g. by using it for direct marketing for its own services. The transport company would then be the data controller. But in most cases a transport company will not be allowed to do that at all. As processor he may only do with the data what the customer asks him to do, and this is usually limited to taking care of the transport and recording it.

The last question is what this division of roles (customer = data controller, transport company = processor) means for the two parties. The most important obligation for the processor (the transport company) is that the processor must adequately secure the data. The data controller (the customer) must record the agreements with the processor regarding the data processing in writing (in a data processing agreement),

[3] *See: https://autoriteitpersoonsgegevens.nl onder het kopje onderwerpen.*

and also check that the processor complies. This particularly applies to the processor's security obligation. As we already indicated in the last paragraph, the transport company may only process personal data on the instruction of the data controller. He thus may not decide independently to effect specific processing of data entrusted to him, unless this is to comply with a legal obligation, e.g. the tax legislation which mandates that the administration must be kept for seven years.
The data controller must ensure that the data is processed in a proper and careful manner, and is thus primarily liable if something does go wrong. But if the mistake lies with the processor in whole or in part, the processor is liable for his part. Lastly, both the data controller and the processor (and their personnel, of course) are subject to a duty of confidentiality with regard to the data entrusted to them.

In summary, we can say that most transport companies in their role as service provider will have little to do with the privacy rules. They will have to sufficiently secure personal data and see to it that they only process the data in conformity with the data processing agreement with the customer. In the light of new privacy rules (see §4) the customers are expected to ask of processors more and more often to demonstrate that they have their affairs in order in the area of privacy.

3.2 The transport company as employer

In their role of service provider transport companies thus do not have that much to do with the privacy rules. The matter is completely different in their role as employer! There are numerous rules for properly dealing with your personnel's data. Naturally the personnel database and the payroll administration must be kept up to date, including with regard to statutory obligations. But there is a lot more: screening of applicants; tracking and monitoring of personnel by means of, e.g., checking emails, internet and telephone use, camera supervision, access passes, GPS or digital speedometer; implementation of rules relating to illness, reintegration and occupational disability; combatting fraud; use of social media, etc. It is beyond the scope of this article to go into this matter in detail, which for the greater part is not specifically intended for transport companies. The website of the Dutch Data Protection Authority contains a lot of information about a number of these specific topics.[4]

4. Developments in the area of privacy

To conclude this article, we will briefly discuss the statutory amendment of 1 January 2016 and the General Data Protection Regulation.

4.1 Statutory amendment of 1 January 2016

As of 1 January 2016 security infringements which have serious negative consequences for the protection of the processed personal data ('data leaks') must be reported to the Dutch Data Protection Authority within 72 hours. In addition, as of 1 January 2016 the Data Protection Authority has the power to impose fines of up to € 820,000 for breaches of all statutory privacy rules. The Data Protection Authority has published policy rules for fines so that insight is provided into how the amount of an administrative fine will be determined.[5] These fines are nothing compared to the maximum privacy fines which are laid down in the General Data Protection Regulation: 4% of the worldwide annual turnover in the preceding financial year, or (yes, you are reading it right) 20 million euros – whatever is highest!

4.2 General Data Protection Regulation

At European level authorities have been working on a General Data Protection Regulation for several years.[6] This Regulation will have direct effect throughout the entire EU as of 25 May 2018. The Regulation is thus a kind of European privacy law, so that national laws like the Dutch Data Protection Act will lapse or may only contain rules which are not contrary to the Regulation. Substantively there will be changes, but the basic principles remain the same. The most important change is in the area of privacy management, the first core obligation under §2.2. Currently this is still an obligation which is buried in the small print in the Dutch Data Protection Act, in the future a number of specific requirements in this area will be added to the Regulation. For example, many larger companies will be obliged to appoint a privacy officer.

5. Conclusion

Transport companies process personal data. In their role as service provider they will generally be data processors. It is important to only use the data in conformity with the data processing agreement for the performance of the contract of carriage and compliance with statutory obligations. Whoever uses the data for their own ends, such as direct marketing, or furnishes the data to others, runs a liability risk. The data must also be properly secured. In their role as employer, transport companies, just like other employers, have to deal with all kinds of privacy rules. With an eye on the substantial fines which can be imposed, it is recommended to keep privacy management in order.

4 https://autoriteitpersoonsgegevens.nl.
5 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebeleidsregels_autoriteit_persoonsgegevens_staatscourant_2016-2043_0.pdf
6 The regulation will probably be adopted in the spring of 2015, which will be followed by a transition period of two years.

Electronic consignment note

Big data and liability

Big data arises because many users store data with a cloud service. The service provider can analyse this data in anonymised form, for example with an algorithm. What rules must a cloud service satisfy and is a cloud service liable for the continuity of its service?

Polo G. van der Putt is an IT attorney with Vondst Advocaten in Amsterdam

1. Introduction

At the beginning of February 2013, the customers of the English cloud provider 2e2 received an alarming letter. The customers, including Vodafone and Citigroup, were summoned to confirm within 24 hours that they would pay up to £ 40,000 extra a week during 16 weeks, because otherwise the continuity of the services could not be guaranteed. The letter came from 2e2 itself, which did not have its finances in order and was on the verge of collapse. The letter also stated that if the first amount were not paid within one week, "we will be unable to continue to provide services to you." According to 2e2 a total of £ 960,000 was necessary to be able to survive. This true example illustrates how dangerous the matter can be for a company to have its data processed by a third party. These kinds of examples raise the question how data processing is regulated by law and what safeguards the law provides.

2. Big data

Because the quantity of data on earth is increasing exponentially and more and more is being stored in the cloud, the question is becoming more and more urgent. Whereas in 2012 worldwide 1.2 ZB in data was stored, it is expected that in 2020 more than 35 ZB will be stored. A ZB (Zettabyte) is equal to 1,000,000,000,000 gigabytes, i.e. approx. 3.4 times the scope of all human knowledge in 2007. The enormous data quantities which are processed these days go under the heading of 'big data'. In this article I will go into the liability for processing big data. I will discuss liability for holding data and liability for the use of data.

3. Statutory duty of care for holding big data

At present the discussions on big data are primarily about the confidentiality of data. This raises questions about the duties of care of the holder of data. In the Netherlands there is no general statutory regulation for information security. A starting point will therefore have to be found in other statutory regulations.

The contract whereby one party holds and/or processes data for the other party, will as a rule qualify as a contract of assignment. The contract of assignment is one of the special contracts from Book 7 Dutch Civil Code (DCC). This entails that the service provider who holds big data pursuant to Art. 7:401 DCC in his business owes the duty of care of a good contractor. This aligns with the criterion for IT service providers developed in the case law: the activities of the IT service provider must comply with the degree of care which can be demanded of a reasonable and competent IT service provider (see inter alia HR 11 April 1986, Computerrecht 1986-3, p. 174 (RBC/ Brinkers)).[1] The case law about the concrete application of this standard is very casuistic. For example, it has been determined in a case that an IT service provider may be expected to evaluate whether the prerequisites are present to meet the customer's requirements. It has also been held that an IT service provider may be expected to warn the customer in writing if he is taking an irresponsible risk. The contents of the duty of care for data processing will therefore primarily be determined by the contract. The precise circumstances and market customers are relevant for the interpretation of the contract. Depending on the text of the contract, the nature of the data and the role and expertise of the parties, there might be a security obligation to a greater or lesser degree. However, there is no case law which provides any further elaboration on this point. It is to be expected that lower (security) requirements will be set for a service provider who 'only' makes storage space available than for a specialised service provider who offers high quality services. In the first case, the service provider is not much more than the lessor of a digital garage.

[1] *See inter alia HR 11 April 1986, Computerrecht 1986-3, p. 174 (RBC/Brinkers)*

The lessee of a garage is given the key and then it's up to him what he does with his garage. Perhaps he will garage his classic car, surplus furniture or old issues of *Weg en Wagen*. Generally the lessor will not have any involvement with the contents of the garage. You cannot expect too much with regard to security. But if the service provider offers services directed at valuable data, more serious requirements can be set. Compare for example the contract whereby a bank takes custody of securities. Tight security will be expected in such a case.

In many cases the data will also relate to persons and the Dutch Personal Data Protection Act is relevant. The Data Protection Act requires that personal data is adequately secured in conformity with the current state of the art. Pursuant to the Dutch Data Protection Act the contract with the service provider must provide for this duty of security. The supervisory body, the Dutch Data Protection Authority, has issued guidelines for the security of data. However, that data does not prescribe any concrete security measures. The guidelines are rather a process description to come to a good security policy.

In short, it ensues from the guidelines that a risk analysis must be carried out and measures must be taken in conformity with market use, for which ISO norms can provide input. For example, information security ISO 27001 is leading. The Dutch Data Protection Act also has a notification duty in relation to data leaks, linked to high fines. There can be a notification duty if someone has left his password lying around. In 2018 the Dutch Data Protection Act will be replaced by the European Data Protection Regulation. This is based on the same principles as the Dutch Data Protection Act, but provides more means. For example, IT systems must provide for functionalities to protect privacy ('privacy by design') and the most privacy-friendly settings are the starting point ('privacy by default').

A contractual security obligation naturally offers an important safeguard, but can naturally never guarantee that the data cannot be viewed or processed by third parties. Certainly if money can be earned with the data, this can attract data hackers. In the end any security can be circumvented. But not only hackers form a threat. If the Snowden matter has taught us anything, it is that national governments also actively search through data, whether or not with the cooperation of the relevant service providers. Companies which wish to reduce the risk of espionage by a foreign government therefore sometimes stipulate that the data may not be stored in certain countries.

Although most attention in the public debate goes to security, the availability of data will generally be of greater importance for the customer. Certainly if the customer is dependent on the availability of his data, the service provider can be subject to a far-reaching obligation to actually keep the data available. The Oilily/Saasplaza case illustrates this.[2] Oilily's company information ran with cloud provider Saasplaza.
Oilily had financial setbacks and obtained a moratorium on payment. At that time it had payment arrears with Saasplaza of approx. € 250,000. Saasplaza announced it was suspending its services. According to Oilily, however, its entire logistics system was dependent on the systems hosted and managed by Saasplaza. Without these systems everyone would lose track of stocks, sales and supplies. In other words, cessation of service would be a deathblow for the company. For these reasons, according to Oilily Saasplaza should not just be allowed to cease its services. Oilily therefore went to the preliminary relief judge to prevent this. The court held Oilily to be in the right, without making it clear, however, on what legal theory this is based:

> *"For the time being it is therefore likely that the services which SaaSplaza provided to the Oilily Group are so essential for business operations [...] that SaaSplaza in the given circumstances cannot simply immediately suspend its obligations. Oilily must therefore in principle be given a reasonable term to prepare for termination of the contractual relationship with SaaSplaza."*

Sight was not lost of Saasplaza's interests. Oilily was to pay an advance for the services to be provided and the obligation to continue services was limited in time. The judgment shows that a service provider is subject to a far-reaching obligations of availability, even with substantial payment arrears.
In connection with availability the question then arises in what degree the service provider must provide back-ups and fall-back options in the event of disasters. In practice, service providers generally take the position that these kinds of continuity measures are additional services, which must be separately agreed and paid.

Service providers thus take the position that continuity measures must primarily be initiated on the part of the customer. A judgment of Amsterdam District Court confirms this basic principle.[3] The matter concerned a consumer who wanted to have her laptop repaired. After the repair all her data turned out to be lost and only an empty operating system was left on the laptop. The applicable general conditions set out that the consumer had to make a back-up. According to the district court the consumer should have done that and could and should have been aware that data and settings could be lost during the repair. The claim for damages was dismissed. A company which places its data elsewhere would therefore be advised to lay down provisions

[2] *Rb Amsterdam, 9 April 2009, case no. 424295 / KG ZA 09-718 (LJN BJ5559), ITenRecht.nl IT 44.*
[3] *Rb Amsterdam 27 February 2013, case no. 1381154 \ HA EXPL 12-29.24*

for availability and continuity in the contract and take measures which reduce the risk of loss.

4. Liability for use of big data

Liability risks of a completely different order play a role in the analysis of big data. Big data sees to it that data is analysed in a completely different manner. This is illustrated by the following examples. More and more people listen to music online. Spotify is a well-known provider. When you log in Spotify suggests music. Messages like "You have listened to "Stormy Weather", you might like this". Or: "Other users in Amsterdam listened to Mahler's 4th, would you like to listen". These recommendations are made in a fully automated manner. Spotify stores so much data that it does a good job of predicting what users will like. Another long existing example is Amazon, the well-known online bookshop. At Amazon you will receive tips in connection with earlier purchases. Amazon used to have an editorial board of literary scientists. The editorial board has been made redundant in the meantime and the tips are calculated by computer. On the basis of purchases of all customers the Amazon computer calculates what other book best fits with this purchasing behaviour. It has turned out that the computer's tips are better appreciated and have a better predictive character than the tips of the literary editorial board.

What is noteworthy in the Spotify and Amazon examples is that for them the links between data are more important than the reason behind them. Only the fact that the buyer of the Transport Law manual always buys the latest Dan Brown is important. The underlying reason, 'the why', is not relevant. That which has proven itself practically leads the way, not an unproven theory. Big data makes it possible due to enormous quantities of data to make connections which otherwise would not be seen quickly.

Naturally the examples of Spotify and Amazon are fairly innocent, wrong tips will not cause vital damage. But what about when, e.g., doctors on the basis of analysis of big data opt for a specific treatment method, without their understanding the underlying reason for the treatment method which has been found. Are they liable if the treatment method turns out to be wrong? Or conversely, are doctors liable if on the basis of an analysis of big data they should have considered a different treatment method, but failed to do so?
The question is thus whether now that there is more data, we should also be deemed to (be able to) know more. And the more we know, the quicker we will make a mistake and the quicker we will be liable. Future case law will tell us the answer.

5. In conclusion

We are becoming increasingly dependent on data. In practice the obligations of the holder of big data will primarily ensue from the contract. A customer would do well to properly address security, availability and continuity. In addition a customer would do well to take practical measures to prevent disruption of this business activities due to the loss or leaking of data as much as possible. For example, a customer can see to it that he himself always has a copy of the data or he can place his data with various service providers. A customer can also decide not to disclose certain confidential data or to avoid certain countries.

How did things end with the 2e2 customers? After receipt of the threatening letter the customers first of all considered to enforce continuation of the services in preliminary relief proceedings, a costly and uncertain road. In the end sufficient customers turned out to be willing to cough up the necessary money and in this manner buy time to remove their data. This is often the way in IT: the interests are so great that litigation offers little prospect of an acceptable solution. Most disputes are resolved practically, whether or not after a financial accommodation.

The Stichting Vervoeradres (= Vervoeradres Foundation) was founded in 1947 by the organisation for carriers (TLN, Transport Logistiek Nederland) and by the organisation for shippers and shippers that transport for their own account (EVO) and by the organisation of inland waterway carriers (NBB)

The Vervoeradres Foundation writes general terms and conditions for agreements of carriage of goods on the road as well as for other logistic agreements. These general terms and conditions, of which the AVC 2002 is well known, take into account the interests of both shipper and carrier. The AVC 2002 also are used in addition to the CMR treaty regarding subjects that are not dealt with in the CMR treaty, such as loading, stowing and unloading the goods and many more practical issues.

The Foundation also acts as a knowledge base on transport law in relation to road transport. In that role the Foundation has legally advised TransFollow on the development of the electronic consignment note in compliance to national law and the eCMR protocol.
The Vervoeradres Foundation answers your questions on the terms and conditions (AVC 2002), and on the eCMR protocol in connection to the TransFollow platform.

www.evo.nl

www.tln.nl

ISSN-nummer: 0920-6191

Postbus 24023, 2490 AA Den Haag **E** sva@beurtvaartadres.nl **I** www.sva.nl **T** 088 552 21 67 **F** 088 552 21 03