**River Information Services**
Electronic Reporting International

# ERI Guide Part II

## Guidance for the protection of data and a Code of Conduct for Electronic Reporting

## Version 2.0

## 31 August 2006

Edited by: Alexander A. de Lijster, Functional advisor Rijkswaterstaat
David Marsh, United Nations Legal Liaison Rapporteur,

## Table of content

1. PREAMBLE ..... 3
2. INTRODUCTION ..... 4
3. DATA CATEGORIES ..... 5
4. THE PURPOSE OF THIS DOCUMENT ..... 6
5. PRINCIPLES ..... 7
6. RECOMMENDED PRACTICES ..... 9
7. CODE OF CONDUCT FOR ELECTRONIC REPORTING ..... 11
8. REFERENCES ..... 13

# 1. Preamble

Recognising that the **protection of personal data** is strictly settled by European and National legislation, it is of the utmost importance that in the exchange of personal data a level of protection is achieved which at least equals the protection resulting from the principles of the Council of Europe Convention of 28 January 1981(ETS 108) for the protection of individuals with regard to automatic processing of data.

In this convention the member States of the Council of Europe as signatories state that:

- considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;
- considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;
- reaffirming at the same time their commitment to freedom of information regardless of frontiers;
- recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples.

Have agreed:
A number of general provisions, basic principals for data protection and transborder data flows as stated in the respective articles of the convention.

In the RIS directive it is clearly stated under paragraph 10 that:
The introduction of RIS will entail the processing of personal data. Such processing should be carried out in accordance with Community rules, as set out, inter alia, in:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Moreover it is stated in Paragraph 10 that:
the introduction of RIS should not lead to uncontrolled processing of economically sensitive data relating to market operators.

The following text should be seen as guidelines to clarify the legal position of the various parties involved in the electronic exchange of data in inland waterway traffic and transport with regard to the protection of personal data.

# 2. Introduction

Information and Communication Technology (ICT) means are rapidly developing into a well accepted way for the exchange of information between governmental agencies and the private sector. It is therefore of the utmost importance that rules for the protection of privacy are under all circumstances clear and unambiguous.

To ensure that an adequate level of data protection is maintained , whilst also a free flow of data across borders and among the parties involved in International Trade and Transport operations is accomplished, these guidelines will constitute the basis for interchange agreements between governments mutually, the private sector and between the private sector and governmental agencies.

Security of personal data includes protection against unauthorised use of, access to or disclosure of personal information, including all measures designed to prevent, detect and enable investigation of unauthorised use, access and disclosure

Electronic reporting or the exchange of data is always done by the owner of the information or by the party appointed by the owner of the data. However this party will act on behalf of the owner and only will provide electronic information to those parties or companies agreed with the owner.

# 3. Data categories

It is perceived that data in any electronic reporting for Inland Shipping will fall into one or more of the following categories:

1 data which does not need to be treated with any element of confidentiality;
2 data which is commercially confidential;
3 data which is personal in nature and must, therefore be maintained in accordance with the EU data protection principles;
4 data which is sensitive personal data and is therefore subject to the more stringent provisions of confidentiality under the EU data protection principles;
5 data which (potentially in addition to falling into categories 2, 3 or 4 above) is subject to national security considerations.

Category 1 data does not need to be kept confidential. An example of this might be as simple as the name of the vessel carrying an (unnamed) cargo.

Category 2 data must be kept confidential and in accordance with general principles of the duty of confidentiality between the commercial trading partners. No harm is caused by it being treated as if it were category 3 data. An example of this category 2 data will be the nature of the cargo and the identified consignee.

Category 3 data must be maintained and can only be disclosed in accordance with the code of conduct as set out in this document.
An example of such data would be the private address of the members of the ship's crew or any passenger.

Category 4 data will also need to be treated in accordance with the code of conduct and must also be subject to the additional protections accorded to such sensitive data under the EU data protection principles. An example of such data would be the ethnic origins of any member of the crew or any passenger.

Category 5 data must be treated in accordance with the higher of the obligations regarding personal data and the requirements of national security regulations of the countries through which the goods in transit pass. An example of such data would be a cargo (such as explosives and other dangerous goods) which might be more vulnerable to terrorist attack.

All electronic data in the above categories will only be disclosed to parties in accordance with annex 1 of this document. For the purposes of this document the term "personal data" encompasses data in the categories 3 and 4 mentioned above.

# 4. The purpose of this document

Definitions:
For the purpose of this document the definitions of the Convention and subsequent directives, unless otherwise indicated, shall apply.

This document contains a number of guidelines which may constitute guidance for the protection of data and the necessary rules of behaviour during the exchange of electronic data respectively electronic reporting in Inland Shipping.

The document is based on the trials and the experiences gained during the implementation of BICS and during the COMPRIS project (Consortium Operational Management Platform River Information Services)

It is the intention of the ERI Expert Group of the RIS Committee periodically, to evaluate the implementation of the various guidelines taking into account the results and consequences for the electronic exchange of information.

To ensure that based on the practical experiences with the implementation of these guidelines, it has been proposed to use a period of 4 years for the evaluation and to decide after this period whether and if so which parts of the Guidelines should be amended.

Upon the advice of the ERI group the RIS Committee will decide to submit proposals for amendments to the Convention.

# 5. Principles

1. Confidentiality and privacy: The parties in the exchange and in particular the owner of the data should have the certainty that confidential information is indeed treated as such. The right to privacy must be assured.

2. Before starting the electronic exchange of data it should be recorded and agreed between the parties exchanging the data for which purpose the respective information will be used and, where appropriate, which of the categories identified in paragraph 1 above applies.

3. The submitted electronic data will only be used for the legitimate and anticipated purpose for which it has been sent. It is to be prevented that such information is forwarded to third parties without the consent of the owner of the information or that the information is used for other purposes than originally has been agreed. The only exception to this principle would be where disclosure is ordered by a competent authority.

4. Each organisation responsible for the generation, maintenance, use, delivery or otherwise processing of data, must ensure the reliability of the data for the purpose of processing and shall take adequate measures to prevent misuse of this data.

5. No systems should exist for the processing of data related to persons and other data subjects which are kept secret from the owners of that data.

6. The responsible parties for the collection of data are liable for the insurance of full compliance with these principles and rules.

7. Reliability: The receiving party should be able to rely on the correctness and completeness of the information supplied.

8. For the supplier of the information it must be clear, understandable, logical and verifiable what information subject to what conditions is relevant for the respective parties and is being used for that purpose (Transparency forms the basis of trust).

9. Personal data can only be submitted to services such as immigration and to security officers on terminals or quays and only in the context of execution of the ISPS code, rules and regulations in those places where the ISPS code is applicable.

10. Personal data should not be kept longer than necessary for the purpose for which the data have been submitted. If the personal data are provided to terminals in the context of ISPS the data will only be kept for the period of stay of the vessel at any terminal.

11. It is not allowed to link personal data from a data subject to the personal data from other data subjects.

12. It should be possible for a person to know which personal data has been gathered for a certain purpose and how this data has been processed.

13. Personal data can only be exchanged after the explicit permission of the person concerned and only to by that person named organisations, companies or authorities for a named purpose. In so far as personal data is passed on to third parties, this shall only be done with the consent of the person concerned or in exceptional cases in accordance with a legal duty.

# 6. Recommended Practices

1. References for the collection of data:

   - correctness and integrity;
   - availability;
   - trustworthiness;
   - non repudiation;
   - authenticity;
   - auditability.

2. Confidentiality

   The majority of the messages that will be transferred will contain information about the location of a ship, data about the ship, the people on board and/or the cargo it is transporting. This information, which may fall into categories 2 and 5 above, can be valuable to competitors, criminals and even terrorists. Thus, the information should be kept secret, except for the receiving party.

   This means that the information might need to be encrypted in such a way that it can only be decrypted by the receiving party; additionally, the sending party should have means to authenticate the recipient in order to avoid communicating the confidential information to an impostor.
   Technical specifications dealing with the details of the security aspects of EDI messages such as for instance the need for common encryption methods will be dealt with separately through the ERI group of experts.

3. Integrity

   The transferred messages need to be protected from unauthorized modification whilst in transit from one system to another. Where required a means will be defined and provided enabling the receiving party to detect whether the message has been altered or corrupted.

4. Non-repudiation

   Message integrity is not only necessary in order to ensure the correct workings of the system but is also a requirement for non-repudiation. Non-repudiation provides proof for the integrity and origin of data, so the sender can be held responsible for the data being sent. It is achieved through for instance cryptographic methods and it prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection or authority (origin) for proof of obligation, intent, or commitment, or for proof of ownership).

5. Verifiability/ audit ability

   Records of all transactions must be kept in such a way that this can support an audit to determine whether all transactions and their processing have occurred as claimed. This might have to include archival of the messages being sent or rejected or received.

6. Information sent only once

   All information concerning a vessel, its voyage, or its cargo should be entered and sent only once. This implies that the server should be able to duplicate information and make it available to other rightful parties as agreed upon here and doing this only when required.

7. Sender is always responsible

   The sender of the information is always responsible for the information being sent. This means that the integrity of the information will need to be guaranteed in all cases. In case of modification of the message (for instance during an EDI translation), this might pose a challenge to ensure that the owner of the information can maintain his responsibility for the correctness of the data.

   The content of an electronic report which does not represent accurate and correct information as a result of force majeure or other circumstances beyond the control of the sender concerned, shall lead to no further action of the receiving authorities, provided that the facts are duly established to the satisfaction of the authorities concerned

# 7. Code of Conduct for Electronic Reporting

1. Upon receipt of electronic information the validity, legal effects and /or enforceability thereof shall not be dismissed on account of the mere fact that the information is electronic. Where it is the intention to report on the status of the ship, the cargo or the persons on board this information shall not be denied on account of the mere fact that this information has not been presented or made available (also) in hard copy.

2. Parties will ensure that where only electronic information is exchanged, the means for the exchange of data are integrated within the organisation. Information and communication systems should be designed in such way that it is possible that obligations undertaken and commitments entered into for the electronic exchange of data can be honoured at all times.

3. Parties shall refrain from activities capable of jeopardizing the availability of electronic information and communication systems. The receiving systems should be organised in such way that the reliability, availability, robustness and timeliness of the information system is assured wherever reasonably possible.

4. Where required and necessary parties shall arrange :
    - what reliable forms and technologies they accept for electronic signatures;
    - what reliable forms and technologies they use for electronic signatures;
    - the verification of an electronic signature;
    - quality standards imposed on third parties;
    - the responsibility for the confidentiality of the electronic signature.

    Third parties whose services might be used for the purpose of the management of electronic signatures shall be required demonstrably to comply with independently set quality standards.

    This means that where applicable the used rules, for instance for trusted third parties should be conform to the European Directive on a community framework for Electronic Signatures (1999/93/EC).

5. The sending party shall clearly indicate whether information in a message is also available for other parties, private as well as governmental taking into account the respect for privacy.

6. In addition to paragraph 5 and in accordance with Annex 1, parties will keep a record which information has been made available for the respective control purposes of governmental agencies and which information may have to be used in case of calamities.

7. A confirmation of receipt of certain electronic information can be part of the agreements between sending and receiving parties.

8. For information received from another party or a third party of which the receiving party may in reasonableness be aware that it needs to be treated as confidential, effective measures should be taken to guarantee that confidentiality is maintained. In principle all information exchanged for the purpose of electronic reporting should be considered confidential unless the contrary has been explicitly indicated by the owner of the information.

9. Agreements about the availability of data will under no circumstances be in contradiction with the aforementioned rules on privacy regarding personal data. Personal data that are no longer required for electronic reporting purposes will be destroyed.

10. All involved parties will protect the information against the possibility of unauthorised changes and should take steps to ensure the audit ability of the sent and received information.

11. Receiving parties should take all necessary steps to ensure that the information received stems from the party that is responsible for the information or where applicable of a party that has obtained the rights to submit the data on behalf of the rightful owner of the information.

12. The captain (skipper) respectively master of a vessel remains responsible for the integrity, correctness and completeness of the information be it in the form of electronic data or otherwise, which is being supplied by him or on his behalf.

13. Where another party supplies the information on behalf of the captain (skipper) respectively master as delegated by him, this party will ensure that the captain (skipper) respectively master is at all times aware of the data content of the respective communication and has the right and obligation to change the information where required in order to execute his responsibilities as the responsible party.

14. In the attachment an overview is given which parties and possibilities there are to support the decisions under which circumstances there is a legal right or a commercial need of certain parties to obtain certain information and under which conditions this information should be made available.

# 8. References

**Applicable directives and sources in no particular sequence**

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28.1.1981 ETS 108
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
- Directive (EC) 7015 / 99 of the European Parliament and of the Council of 25.04.1999 on a common framework for electronic signatures.
- OECD Guidelines on the protection of Privacy and Transborder Flows of personal data
- ICC Guidelines for commitments on privacy protection by access providers and website operators
- UNCITRAL Model law on Electronic Commerce 1996