Protection of personal data when using Inland AIS devices

Summary report: review of national regulations as at 15 April 2014

1. Review of current data protection regulations pertaining to Inland AIS

1.1. In Switzerland, data protection is regulated at federal level by the Federal Data Protection Act (DPA), RS 235.1) of 19 June 1992 and by the Ordinance to the Federal Act on Data Protection (ODPA), RS 235.11) of 14 June 1993. This Act aims to protect the personality and fundamental rights of persons whose data are being processed. As Inland AIS does not transmit personal data as construed in the Swiss Act and, as such, does not generate any personality profiles, the DPA does not apply to data transmitted by Inland AIS devices.

Likewise, data transmitted by Inland AIS devices is not subject to specific regulations in Switzerland.

On the other hand, the Swiss Penal Code contains a number of provisions which might be invoked by boat masters were third parties to intercept or make fraudulent use of data transmitted by the Inland AIS device without their consent. The principal articles likely to be invoked are:

- article 143 which combats "*data misappropriation*".

  This means that whoever, with the intention of procuring for themselves or a third party an unlawful enrichment, shall have misappropriated for himself or a third party, data that has been recorded or transmitted electronically, or by a similar method, which was not intended for him, and which was specially protected against any undue access on his part, shall be punished by a maximum penalty of five years of imprisonment or a fine. Data misappropriation committed to the detriment of relatives or family members will only be prosecuted in response to a complaint.

- Article 143^{a} which penalises *undue access to an IT system*

  It states that any individual who, without authorisation, uses a data transmission device to gain admission to an IT system belonging to someone else, and which was specially protected against any access on his part, shall, in response to a complaint, be punished by a maximum penalty of three years of imprisonment or a fine.

- Article 144^{a} which punishes "*damage to data*"

  Point 1 of this article states in particular that anyone who, without authorisation, modifies, deletes or renders inoperative data recorded or transmitted electronically, or by a similar method shall, in response to a complaint, be punished by a maximum penalty of three years of imprisonment or a fine.

1.2. In France, data of a personal nature are afforded special protection, in particular when being processed, otherwise expressed when they are contained, or required to be held, in files. Current rules for protecting personal freedom therefore aim to regulate the circumstances in which public and private individuals may create files containing information of a personal nature (Law No. 78-17 of 6 January 1978 pertaining to Information Technology, files and liberties and Decree No. 2005-1309 implementing the aforementioned Law). The French National Commission for Data Protection and Liberties (CNIL), an independent administrative authority, provides this protective role. It is consulted on any draft text pertaining to the protection of individuals as regards automated data processing. It is also involved prior to the implementation of this sort of processing, either to authorise it or to provide a reasoned opinion on the processing being contemplated. Finally, the CNIL also exercises investigatory, supervisory and punitive powers.

1.3. In Belgium, the Law of 8 December 1992 relating to the protection of private life as regards data of a personal nature, has underpinned the regulations on the protection of personal data (Royal Decree of 13 February 2001, implementing the Law of 8 December 1992 concerning the protection of private life regarding the processing of data of a personal nature). What is meant by data of a personal nature is: “any information relating to an identified or identifiable physical person, hereinafter referred to as “person concerned”; a person shall be deemed to be identifiable if he can be identified, directly or indirectly, in particular by reference to an identification number or to one or a number of specific items of information, peculiar to his physical, physiological, psychological, economic, cultural or social identity. ”

An independent supervisory body to the Chamber of Representatives was instituted on 1 January 2004 : the Commission for the Protection of Private Life. Its remit is to ensure that private life is respected when processing data of a personal nature. It examines any complaint in parallel with the procedure carried on by the court of law. It will play a mediation role to effect a reconciliation between the parties or, in the absence of a reconciliation, it will hand down an opinion.

1.4. In the Netherlands the legal system is based on two tools: the Maritime and River Navigation Code Concerning the Protection of Personal Data (Wbp)

- Measures for waterway users are based on the *“Scheepvaartverkeerswet”* (Maritime and River Navigation Code). It features a framework allowing for delegation of the regulations regarding*“the receipt, retention and communication of navigation-related data by organisations and persons who are not involved in traffic*”. (Article 4(1)(E)).

  This article provides inter alia for the ability to regulate the receipt, processing and reuse of information in the context of River Information Services (RIS)[1], including persons / organisations ashore.

  Other rules are stipulated by Order in Council, notably the resolution concerning reporting formalities and the processing of navigational data.

- The processing of personal data is governed by the Personal Data Protection Act (Wbp).

1 defined in article 1(1)(p) of the Code by the following form of words : “harmonised information services promoting traffic and transport management in the navigation arena, including, wherever technically possible, interfaces with other modes of transport or other commercial activities that are not internal commercial activities between one or a number of the companies concerned. ”

1.5. In Germany, the legal system essentially exists on two levels:

- framework legislation (The Federal Data Protection Act and the corresponding laws of the Laender)

- data protection laws specific to the area in question. Inland navigation law also comprises provisions relating to data protection that are specific to certain areas, for example in the so-called *Binnenschifffahrtsaufgabengesetz* (law determining the extent of obligations pertaining to inland navigation), which regulates a number of databases (infringements, fleet vessel inventory etc.) but contains no provisions as to Inland AIS. Indeed, as of now, there are not yet any specific regulations on the protection of AIS data.

- The competent authority at federal level for data protection-related issues is the "Federal Commissioner for Data Protection and Information Security". As concerns penalties in the event of data misuse, authority resides with the public ministries or agencies appointed by the various data protection laws.

2. What measures have been taken to protect personal data transmitted by the Inland AIS device and their use (non-commercialisation, processing...)?

2.1. The Swiss delegation proposes providing the profession with exhaustive information on what data is gathered, how long it will be retained and precisely what use is made of these data, with a view to securing its approval. As a result, these aspects should be taken into consideration in the CCNR resolution.

2.2. The procedure followed in France for Inland AIS devices is the "standard" declaration provided for in article 23 of Law No. 78-17 of 6 January 1978 concerning current processing practices. This declaration includes the undertaking that the data are being processed as required by law. What data are transmitted is stipulated in article 30 of the aforementioned law. The applicant may process the data upon receipt of the voucher issued by CNIL.

Other data protection measures are in place:

- protection of physical access to the processing,
- implementation of a user authentication procedure,
- the logging of connections,
- data are processed within a dedicated internal network (not connected to the Internet),
- the transport channel is encrypted for data exchanged on the Internet network.

The likely destination organisations are as follows: the carriers, the shippers, the in-house departments of VNF (French Waterways), the customs, river police, justice departments, third parties authorised by the seaman himself.

2.3. In Belgium, article 17 of the Law of 8 December 1992 referred to in 1.3 prescribes the procedure to be followed when processing data. It therefore applies to Inland AIS device data. Data processing must be subject to a declaration to the Commission for the Protection of Private Life. Section 3 of article 17 details the data that must be included in the declaration.

2.4. In the Netherlands, the measures that have been enacted flow from the two reference texts;

a) As regards any information gathered in connection with the reporting requirement and for any information received in connection with the RIS, articles 7, 8 and 9 of the resolution in relation to reporting formalities and the processing of navigational data stipulate who may receive this information and in which circumstances. Under the terms of these articles, the local waterway manager is allowed to use the information for traffic management purposes. However, the waterway manager or anyone else is expressly forbidden from availing themselves of these data to verify compliance with the regulations, unless an infraction is suspected.

This protection extends to all navigation data used for traffic management. This covers not just RIS data but also information received via reports, mandatory or otherwise, for example the reporting requirement referred to in article 12.01 of the RPR and information obtained via a radar image from a shore facility by means of which the route taken by a vessel is recorded.

In conclusion, any infringement of the resolution as regards reporting formalities and the processing of navigational data is punishable under article 31(4) of the Maritime and River Navigation Code. This provision provides for the imposition of a punishment in the form of imprisonment or a fine up to a maximum of 7,800 euros per offence.

b) If organisations or persons do not fall within the scope of the resolution mentioned in 1.4, or if the data does not originate from traffic management, two legal instruments afford protection for data from Inland AIS devices:

- The first is the Penal Code. Any divulging of information by a person who has obtained this information when it was not intended for him shall be deemed to be a breach within the meaning of article 441 of the Penal Code. Depending on what use has actually been made of the information obtained (for example if the information is disclosed), any misuse may be punished in accordance with this article.

- The Personal Data Protection Act may also be invoked in certain circumstances. Indeed, AIS information can often be associated with physical persons as many waterway undertakings are sole traders. In this case the data are personal. According to the legal department of the Ministry of Infrastructure and the Environment and the Council for the Protection of Personal Data (CPB), AIS information is deemed to be personal data, because in many cases in inland navigation, these data can be associated with individuals. That means that the disclosure, sale etc. of AIS data, without the sender's explicit consent – provided they can be associated with physical persons – are very probably governed by the WBP.

The purpose of numerous provisions of the WBP is the interest of the persons in question, such as article 8, stipulating the situations in which personal data may be processed. The CPB may impose a fine, or the judge in a criminal court may impose a prison sentence, if organisations or persons ashore fail to abide by these requirements when processing data transmitted by the Inland AIS.

2.5. Under German law, AIS data are personal data, as the data are capable of being associated with a person. Consequently, from a data protection perspective:

a) If the authority wishes to use data transmitted by the AIS for traffic management purposes, it needs to set up an accredited database specific to the area, defining in detail what data may be gathered, recorded and disclosed, as well as their permitted use.

b) On the other hand, the introduction of the compulsory possession and use of AIS equipment for automatic signalling between boat masters requires no new legal data protection framework.

c) Requirements already in force enable AIS data to be protected against third parties, unrelated to navigation, who might wish to use it in a way that is not desired. Article 202b of

the penal code punishes “data interception” and article 43(2) (1) of the Federal Data Protection Act protects personal data that are not universally available against being gathered and used.

3. Amendment / development of the regulations / legislation

3.1. No amendment / development of current regulations is currently envisaged in Switzerland, France, Belgium or the Netherlands.

3.2. In Germany this year, the Federal Ministry of Transport and Digital Infrastructure has planned to launch a legislative initiative to amend the so-called Binnenschifffahrtsaufgabengesetz so that AIS data may in future be used by the authorities. The draft legislation should be completed by the end of 2014.

3.3. The French, Dutch and Belgian delegations have also pointed out that European Directive No. 95/46/EC of 24 October 1995 constitutes the current European data protection framework. A reform currently in hand aims to take this framework to the next level by replacing it with a European implementing Regulation in all the Member States of the European Union. The aim of this text is to achieve better harmonisation and make personal data protection more effective.

***