INTERNATIONAL MARITIME ORGANIZATION

IMO

E

SUB-COMMITTEE ON STANDARDS OF TRAINING AND WATCHKEEPING
36th session
Agenda item 4

STW 36/4/1
19 July 2004
Original: ENGLISH

UNLAWFUL PRACTICES ASSOCIATED WITH CERTIFICATES OF COMPETENCY

Revised reporting format on fradulent certificates

Note by the Secretariat

SUMMARY

Executive summary:	This document provides the legal implications relating to the protection of personal data and the implications for the Organization in publishing such information.
Action to be taken:	Paragraph 5
Related documents:	STW 35/19

1 The Sub-Committee, at its thirty-fifth session (26 to 30 January 2003), discussed the suggestion that the name of the individual holding a fraudulent certificate and his/her passport number or other identification details should also be included in the report and published by the Secretariat, in a revised format. The Sub-Committee noted that this information would be of interest to Member States and thus allow them to assess the need for any further action.

2 The Sub-Committee agreed that before it could make a decision on the provision of details of the identity of the individuals involved, there was a need to examine the legal implications, particularly in connection with provisions of international treaties and national legislation relating to the protection of personal data and the implications for the Organization in publishing such information. In this respect it was noted that at the international level, amongst others, Article 12 of the Universal Declaration of Human Rights, the United Nations Guidelines concerning Computerized Personal Data Files (adopted by the UN General Assembly on 14 December 1990) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, contained provisions to this end.

3 The Sub-Committee instructed the Secretariat to study the matter *vis-à-vis* the position of, and the implications for the Organization if such information were to be published, and advise the Sub-Committee accordingly (STW 35/19, paragraphs 5.10 to 5.13).

4 The Legal Division of the Secretariat has examined the position of, and the implications for the Organization if such information were to be published and its advice is set out in the annex.

Action requested of the Sub-Committee

5 The Sub-Committee is invited to note the information provided and take action as appropriate.

***

ANNEX

ADVICE FROM LEGAL DIVISION

1 The STW Sub-Committee is in the process of developing a format for the reporting of information provided to the Secretariat on fraudulent certificates. Currently, the report contains the name of the country which reported discovery of a fraudulent certificate, the flag of the ship on which the certificate was discovered, the country which is identified as having issued the certificate, and the date on which it was discovered, along with general comments. A proposal has been made to include the name of the individual holding the fraudulent certificate as well as a passport number or other personal identification details. Concern was expressed, however, there might be legal implications to the publication of such personal information by the Organization. It is also unclear what purpose would be served by including personal information in a report which is apparently to be generated once a year to inform the Sub-Committee of the reported scope of the problem with fraudulent certificates. (It is understood that this reporting system is separate and distinct from the web-based system operated by IMO as a portal to allow user access to national certificate databases for determining whether individual certificates are valid.)

2 A limited but broad survey of laws and guidelines pertaining to systems in which personal data is recorded indicates that there are a number of common principles and elements intended to protect the privacy of the individuals concerned. These include the following:

.1 **Right to privacy:**

Universal Declaration of Human Rights (article 12): "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

USA Privacy Act (section 552): "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to a range of other specific exceptions]."

.2 **Principle of accuracy:**

UN Guidelines Concerning Computerized Personal Data Files (adopted by the General Assembly on 14 December 1990) - Section A.2 : "Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed."

.3 **Principle of Interested-Person Access:**

UN Guidelines Concerning Computerized Personal Data Files: "Everyone who offers proof of identity has the right to know whether information concerning him

is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, addressees. Provision should be made for a remedy, if need be with the supervisory authority… The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence."

USA Privacy Act: "Each agency that maintains a system of records shall-- (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence; (2) permit the individual to request amendment of a record pertaining to him and…promptly, either-- (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official; make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process [and] establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records."

.4 **Application of the guidelines to personal data files kept by governmental international organizations:**

UN Guidelines Concerning Computerized Personal Data Files: "The present guidelines should apply to personal data files kept by governmental international organizations, subject to any adjustments required to take account of any differences that might exist between files for internal purposes such as those that concern personnel management and files for external purposes concerning third parties having relations with the organization. Each organization should designate the authority statutorily competent to supervise the observance of these guidelines."

.5 **Data Security:**

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28 January 1981) -- Article 7: "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."

Additional safeguards for the data subject: "Any person shall be enabled:

(a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

(b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

(c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

(d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."

3 The point of the above survey is to indicate the complexity of the law which is developing around record-keeping systems and the protection of personal privacy, and to suggest the types of burden that are placed on the manager of a data base to ensure that it is accurate. It may well be possible to craft a caveat or disclaimer to protect the Organization from legal liability for errors in the proposed recording-keeping system on fraudulent certificates; however, unless the identification of individuals would demonstratively and directly promote compliance with or enforcement of IMO conventions in a way which cannot be accomplished by some other means, and unless the criteria for determining whether a particular certificate is in fact fraudulent are uniformly applied, and unless there is a reliable means of guaranteeing that such records will be kept up-to-date and accurate, the Legal Division cannot recommend that personal information be maintained in a data base which is to be managed by the Organization for preparing a periodic report to the STW Sub-Committee.

_____