

INFORMATION SHEET ON PROCESSING AND PROTECTING GENETIC AND OTHER PERSONAL DATA

Reference: ICMP.POL.DG.04.doc

WHAT IS PERSONAL DATA?

Personal data is any information relating to an individual human being. This may include a person's name, date and country of birth, and gender. Sensitive personal data refers to personal data that indicates race, ethnic origin, religious, philosophical, or political association, or other potential grounds for discrimination. Genetic data, that is a person's DNA, always constitutes sensitive personal data.

WHY DOES ICMP ASK FAMILY MEMBERS TO PROVIDE PERSONAL DATA?

ICMP asks family members of missing persons to provide personal data, including DNA, to assist government institutions and other authorities to account for missing persons. DNA may be necessary to identify mortal remains of missing persons. DNA can also be used to reunite children with their families if they have been separated, or to locate victims of trafficking.

WHAT DOES ICMP DO WITH PERSONAL DATA?

ICMP combines personal data about missing persons provided by relatives with data obtained from other sources. For instance, a photograph of a missing person provided to ICMP by a family member, combined with information from someone who has seen the person, can lead to locating the missing person. ICMP collects blood or saliva samples from family members and extracts DNA, which is then compared through a mass database with DNA extracted from unidentified human remains. When there is a DNA match, it is possible to make a conclusive identification.

Many sources may hold data relevant to locating missing persons. These sources may also hold data concerning family members themselves. ICMP does *not* search data sources for information on family members. Automated searches are automatically prevented from combining personal data from other sources with family members' personal data in a manner that would identify the family member.

ICMP may use personal data to support other international organizations or government institutions in the exercise of their functions. ICMP will transmit personal data of family members to other organizations or institutions only with the free, informed and express consent of family members who are capable of expressing such consent.

ICMP may share personal data of missing persons that is not sensitive with other international organizations, government institutions and the public. ICMP will not process personal data provided by a family member in the event that the family member objects to sharing of the missing person's non-sensitive personal data.

HOW DOES ICMP PROCESS PERSONAL DATA?

ICMP uses a dedicated data processing system to store and analyze data on missing persons and their family members, including their genetic data. The Integrated Data Management System (iDMS) is operated on ICMP's own data servers at ICMP Headquarters in The Hague. ICMP also uses an

IMPORTANT NOTE: Hardcopy of this document will be considered uncontrolled unless labelled otherwise. It may be used for the operation related purpose of ICMP staff and cannot be further distributed or amended.

online platform called the Online Inquiry Center (OIC). The OIC is an interactive reporting and search tool that allows family members and others to obtain and provide information on missing persons.

Missing persons may have been seen alive. Families can publish a photograph of their missing persons on the OIC's MyFace page. The photograph can be seen by anyone who accesses MyFace, and anyone who may have seen the missing person can provide information on the person's whereabouts by clicking on the photograph. Such information will not be visible to the public.

WHAT PROTECTIONS DOES ICMP GIVE TO PERSONAL DATA?

Data protection is the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the collection, storage, use and disclosure of personal data. To guard against the various risks associated with personal data processing – such as accidental loss of data, theft, manipulation or other forms of unauthorized processing – ICMP has adopted data protection measures that enable family members to control their personal data.

Family members have the right to withdraw, amend or correct their personal data. In the event that genetic and other personal data form part of official conclusions, such as in a family reunification or the identification of the mortal remains of a missing person, such personal data can no longer be withdrawn by the family members concerned.

The iDMS and OIC in particular have been designed to ensure a high degree of control over access to sensitive personal data. Data administrators, including DNA analysts, have access to data only on a "need to see" basis. Sensitive personal data, in particular DNA samples and profiles, are processed in an anonymous, coded form. The iDMS operates automated controls to ensure that personal data is not retained beyond its useful life. For instance, once all persons reported missing by a family have been accounted for, personal data on ICMP servers will be deleted within a specified period of time.

As a treaty-based intergovernmental organization, ICMP benefits from privileges and immunities that guarantee international legal protections of data, and the database and data processing systems.

FURTHER QUESTIONS

For further information about data processing and protection, please contact ICMP at icmp@icmp.int or visit the ICMP website at www.icmp.int.