circular

Office of the Director
Bureau du Directeur

Circular No. **DIR 03/2019** Date: **04/07/2019**

International **Training** Centre
Centre international de **formation**
Centro Internacional de **Formación**

Protection of Personal Data

Introduction

1. The Centre collects and processes personal data in a wide variety of contexts, including for the provision of services to constituents or the general public, as well as in the administration of the employment relationship with its officials and in connection with the contractual arrangements entered into with other individuals and entities.

2. This Policy aims to ensure that the Centre is open and transparent in obtaining and using personal data for intended purposes, while safeguarding the rights of individuals to the privacy of their personal information.

3. This Policy is issued further to article V of the Statute of the Centre, which delegates overall responsibility to the Director of the Centre for the efficient conduct of the Centre.

4. This Policy is effective as of the date of issue.

Definitions

5. For the purposes of this Policy, the following definitions apply:

   a) "personal data" refers to information which can be used to identify an individual, either directly or indirectly, such as name or national identification number, passport number, telephone number, residential address, email address, bank account number, employee number, Internet protocol (IP) address, or some other unique identifier pertaining to an individual or any information that when combined, can be used to identify an individual;

   b) "sensitive personal data" refers to personal data which form part of the core area of private life, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well health status (including medical, biological, or biometric data), financial or family/relationship situation (including marital status, sexual orientation and dependents). Sensitive data also include aspects of employment records of Centre officials, in particular those relating to their performance and conduct;

   c) "use of personal data" includes any operation or set of operations which is performed in relation to personal or sensitive personal data, by manual or automatic means, including collection, recording, copying, storage, accessing, retrieval, organization, modifying, dissemination, transmission, disclosure, erasure or destruction.

Scope

6. This Policy applies to any personal data, including sensitive personal data, held by the Centre or by third parties on behalf of the Centre.

7. Standard personal data held by the Centre includes data received from constituents, participants in Centre meetings, staff members, interns, consultants, suppliers, contractors or other individuals associated with the Organization and required for the Centre to comply with its statutory obligations, any other legal basis specifically identified by the Centre in connection with its mandate, and to carry out its related administrative functions. Personal data of other individuals, such as users of Centre websites and other information resources, may also be held and used by the Centre, as required, to provide the service requested.

8. The use of sound and image data, such as in cases of audio and video records, including video surveillance, fall outside of the scope of this Policy.

Policy

9. Personal data shall be processed for specified purposes, which are consistent with the mandate of the Centre and take into account the balancing of relevant rights, freedom and interests. Personal data should not be processed in ways that are incompatible with such purposes.

10. The following principles govern the use of personal data by the Centre. Personal data shall be:

    - obtained for one or more authorized purposes, such as to administer the entitlements of Centre officials, fulfil a contract or meet other legal obligations;
    - processed in a fair manner, in accordance with its mandate and governing instruments ;
    - adequate, relevant and limited to the specified purpose for which they are obtained;
    - accurate and, where necessary, kept up to date;
    - used in a manner consistent with the purpose for which they are obtained and in compliance with the Centre's accountability framework[1], including the Centre Staff Regulations and the *Standards of Conduct for the International Civil Service*;
    - used in accordance with the rights of the individuals concerned;
    - used only by authorized individuals on a "need to know" basis; and
    - subject to reasonable security safeguards, including higher protection measures for confidential information[2].

[1] *DIR 02/2015 Accountability Framework,* of 2 February 2015.

[2] For a classification of information and data, see ICTS 02/2017 *Information Technology Use Policy*, of 1 January 2017.

11. Personal data shall not be:

- with the exception of developing future courses or improving current ones, be used for any for-profit purposes;
- kept longer than is necessary; and
- transferred to another jurisdiction without authorization or without ensuring that such personal data will enjoy sufficient protection under the regulatory framework of that jurisdiction or through the contractual arrangements with the concerned individual or entity.

12. Sensitive personal data shall not be released to third parties without the explicit written consent of the individual concerned, except where required by national law enforcement authorities or competent international organizations, whether in the context of judicial proceedings or where necessary to protect the interests of the Organization or of the individual.

Roles and responsibilities

13. The following roles and responsibilities have been established for implementing this Policy.

Personal data protection function

14. The personal data protection function is devolved to the Human Resources Services, in consultation with Office of the Legal Adviser (JUR), which shall be responsible for:

- developing and reviewing all personal data protection policies and related rules and procedures on a regular basis;
- ensuring that appropriate governance procedures are in place to safeguard personal data and their use with a view to ensuring that they are protect against or from unauthorized or accidental access, damage loss or other risks presented by data processing;
- ensuring the communication of policies, rules and procedures to staff;
- responding to inquiries and questions on personal data protection;
- obtaining the consent of individuals where disclosure of their personal data is contemplated;
- ensuring that any request for the communication or disclosure of personal data to third parties is legitimate, and approving, where required, such communication or disclosure without the consent of the individual concerned; and
- approving any personal data protection and privacy statements attached to communications such as emails, broadcasts and announcements.

Chief Information Officer

15. The Chief Information Officer is the official responsible for ensuring that IT systems used to electronically store personal data have the necessary IT controls in place to securely protect such data. The responsibilities of the Chief Information Officer include, among other things:

- ensuring that all systems, services and equipment used for storing, processing and accessing personal data meet minimum best practice security standards (it being understood that the Centre cannot guarantee that unauthorized third parties will never access personal data);
- performing regular information security checks and scans to ensure hardware and software used to process personal data is functioning properly and complies with Centre information security standards;
- evaluating any third-party IT service provider which may need to use personal data held by the Centre; and
- as necessary, determining other technical standards.

CENTRE officials

16. All staff members are responsible for:

- providing timely and accurate information about any change to their personal data held by the Centre;
- keeping confidential any personal data or sensitive personal data to which they may have had access in the performance of their official duties, including through ensuring that they are electronically and physically secured at all times; and
- reporting swiftly any unauthorized disclosure of personal data.

Requests for access

17. Any individual in respect of whom the Centre holds personal data is entitled to:

- ask what information the Centre holds and why;
- ask how the Centre processes their personal data, including retention and deletion;
- ask how to gain access to their personal information;
- be informed on how to keep personal information up to date; and
- be informed on how the Centre is meeting its personal data protection obligations.

Remedies in case of misuse of personal data

18. Protection of personal data in accordance with this Policy forms part of the terms and conditions of employment within the meaning of article 12.2 of the Staff Regulations. Accordingly, any breach of personal data of an Centre official is subject to the conflict resolution mechanisms provided for in Chapter XII of the Staff Regulations.

19. Claims by any other individual that their personal data held by the Centre has been used in a manner incompatible with this Policy shall be reported in writing to HRS (HRS@itcilo.org) for appropriate follow-up.

20. Queries regarding this Policy should be addressed to HRS.

Yanguo Liu