office directive

IGDS Number 457 (Version 1)

International Labour Office

15 January 2016

Protection of personal data

Introduction

1. The ILO 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 Directive aims to ensure that the ILO 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 Directive is issued further to article 8 of the ILO Constitution which delegates overall responsibility to the Director-General for the efficient conduct of the Office.

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

Definitions

5. For the purposes of this Directive, 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, 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 some employment records of ILO officials, such as 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 Directive applies to any personal data, including sensitive personal data, held by the ILO or by third parties on behalf of the ILO.

7. Standard personal data held by the ILO includes data received from constituents, participants in ILO meetings, staff members, interns, consultants, suppliers, contractors or other individuals associated with the Organization and required for the ILO to comply with its constitutional obligations and to carry out its related administrative functions. Personal data of other individuals, such as users of ILO websites and other information resources, may also be held and used by the ILO, 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 Directive.

Guiding principles

9. The following principles govern the use of personal data by the ILO. Personal data shall be:

   - obtained for one or more authorized purposes, such as to administer the entitlements of ILO officials, fulfil a contract or meet other legal obligations;
   - adequate, relevant and not excessive for the purpose for which they are obtained;
   - accurate and kept up to date where required;
   - used in a manner consistent with the purpose for which they are obtained and in compliance with the ILO's accountability framework, [1] including the ILO 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]

10. Personal data shall not be:

    - used for any commercial purposes;
    - kept longer than is necessary; and
    - transferred to another jurisdiction without authorization and without ensuring that such personal data will enjoy sufficient protection under the regulatory framework of that jurisdiction.

[1] Director General's Announcement, *ILO accountability framework*, IGDS No. 137 (version 1), of 15 January 2010, and Office Guideline, *The ILO accountability framework: Key standards and mechanisms*, IGDS No. 195 (version 1), of 25 October 2010.

[2] Office Directive, *Classification of ILO Information Assets*, IGDS No. 456 (version 1), of 5 January 2016.

11. 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

12. The following roles and responsibilities have been established for implementing this Directive.

Personal data protection function

13. The personal data protection function is devolved to the Office of the Legal Adviser (JUR), which will be responsible for:

- developing and reviewing all personal data protection policies and related procedures on a regular basis;
- ensuring that appropriate governance procedures are in place to safeguard personal data and their use;
- ensuring the communication of policies and processes 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.

IT Security Officer

14. The IT Security Officer is an official in INFOTEC 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 IT Security Officer include:

- 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 ILO 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 ILO information security standards; and
- evaluating any third-party IT service provider which may need to use personal data held by the ILO.

ILO officials

15. All staff members are responsible for:

- providing timely and accurate information about any change to their personal data held by the ILO;
- keeping confidential any personal data or sensitive personal data to which they may have had access in the performance of their official duties; and
- reporting swiftly any unauthorized disclosure of personal data.

Requests for access

16. Any individual in respect of whom the ILO holds personal data is entitled to:

- ask what information the ILO holds and why;
- 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 ILO is meeting its personal data protection obligations.

Remedies in case of misuse of personal data

17. Protection of personal data in accordance with this Directive forms part of the terms and conditions of employment within the meaning of article 13.2 of the Staff Regulations. Accordingly, any breach of personal data of an ILO official is subject to the conflict resolution mechanisms provided for in Chapter XIII of the Staff Regulations.

18. Claims by any other individual that their personal data held by the ILO has been used in a manner incompatible with this Directive shall be reported in writing to JUR (JUR@ilo.org) for appropriate follow-up.

19. Queries regarding this Directive should be addressed to JUR.

Guy Ryder
Director-General