Code of Conduct for the Protection of Personal Data (GDPR)

Index:

1. Aim 3
2. Scope 4
3. Principles of Privacy, Lawfulness of Processing and Data Subject Rights 4
4. Records of processing activities 5
5. Data protection by design and by default 6
6. Security of processing and use of IT resources 6
7. Personal data breaches 7
8. Professional secrecy 7
9. Information and Training 8
10. Clarifications and filling of gaps 8

The Ministry of Foreign Affairs (MFA) is responsible for the processing of personal data, both of its internal human resources, at Portugal and abroad, and of external entities whose data is managed by the MFA.

For the execution of such processing, the MFA complies with the requirements established in the General Data Protection Regulation (GDPR) on the protection of natural persons regarding the processing of personal data and free movement of such data, in force since May 24th, 2016.

Since May 25th, 2018, every organization is inserted in a self-regulated system, and must therefore demonstrate strict compliance with the new legal obligations.

Hence, in accordance with what is established by the articles 40 and 41 of the GDPR, the adoption of Codes of Conduct by the organizations constitutes an important tool to achieve adequate levels of effectiveness and consistency in the protection of personal data.

1. Aim

1.1 The purpose of this document is to define the MFA's Code of Conduct for the Protection of Personal Data, as a set of principles and guidelines that shall govern the actions of all MFA employees, officials, and managers with respect to the protection of personal data.

1.2 Personal data is information relating to a natural, identified or identifiable person. Also considered personal data is the collection of separate information that can lead to the identification of a particular person.

1.3 Personal data that have been de-characterised, encoded or pseudonymised, but which can be used to re-identify an individual, remains personal data and falls within the scope of the GDPR.

For this purpose, examples of personal data are

- name and surnames;
- a home address;

- a personal email address such as name.surname@company.com;
- the number of an identification card;
- location data (e.g. the location data function on a mobile phone)[1]
- an IP (internet protocol) address
- connection details (cookies);
- your phone's advertising identifier;
- data held by a hospital or doctor which uniquely identifies a person

2. Scope

This Code of Conduct stems from the MFA's Privacy Policy and applies to the entire organisation, including employees, officials, and managers of the Internal and External Services.

This Code covers the entire organisation transversally, namely the work methodologies and processes involving the processing of personal data, as well as the use of materials or equipment, programmes or software, communication channels and paper supports.

Thus, it applies to both automated and manual data processing regardless of how personal data is stored.

3. Principles of Privacy, Lawfulness of Processing and Data Subject Rights

With reference to the MFA's Privacy Policy, in performing the tasks assigned to them, all employees, officials and managers of the MFA are obliged to respect the principles of privacy, to ensure that the processing of personal data is within the lawfulness grounds established and that the rights of the data subjects are duly respected.

[1] It should be noted that in some cases there is specific sectoral legislation regulating, for example, the use of location data or the use of cookies - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1)

Accordingly, the MFA's employees, officials and officers shall adopt a set of general good practices in personal data processing operations, ensuring:

- That each processing is carried out only within the scope of the purposes for which the data was collected.
- That the collection, use and storage of personal data is carried out only on the minimum personal data, necessary and sufficient for the respective purpose.
- That personal data is only stored for the period of time necessary to fulfil the purpose for which it was collected.
- that no personal data is transmitted for commercial or advertising purposes.
- That the processing of personal data is carried out for legally established purposes or for the pursuit of requested online services.
- that, in the event of data sharing being necessary, means are used to enable access to be traced.
- that data that is not strictly necessary is deleted.
- That data is kept as centralised as possible in order to be able to fulfil the rights of the data subjects in an agile manner.
- That records of data processing are created or tools and platforms that have such records are used.
- That all and any documents and physical supports containing personal data are kept in a safe and confidential place.
- That access to documents containing personal data is controlled.

4. Records of processing activities

As the controller of personal data, the MFA is obliged to keep a record of such processing containing a range of information, as set out in the Privacy Policy.

These records are kept by the Privacy Officer of each organic unit, appointed for this purpose, and it is the duty of all employees, officials and officers of the MFA to inform the said Officer of any updates to the record that may be necessary as a result of the performance of their duties.

5. Data protection by design and by default

Whenever, in the course of their duties, an employee, official or manager of the MFA collaborates in the development of any process or procedure involving the processing of personal data, they shall take into account the principles of data protection and include the necessary safeguards to ensure that the processing to be carried out complies with the requirements of the GDPR and protects the rights of the data subjects.

6. Security of processing and use of IT resources

The MFA implements the necessary technical and organisational measures to ensure a level of security appropriate to the risk.

The security measures implemented, as well as the principles that guide the MFA's actions in this area, are detailed in the Security Policy and should be taken into account by the MFA's employees, officials and managers.

The conditions of access and use of IT resources by the Ministry's employees, officials and managers are set out in the respective "Internal Rules for the Use of IT Resources".

All data relating to individuals, whether on paper or in computerised, electronic or other form, are covered by the data protection regime.

When transmitting personal data in response to questions from entities or persons outside the ministry, by telephone or email, data on, for example, marital status, personal contacts, addresses, household, among others, shall not be disclosed.

Paper documents containing personal data shall be kept in closed spaces (cupboards, drawers, filing cabinets) and should not be displayed on desks when staff are not working on them.

The filing rooms of the various departments of the MFA shall be kept locked when not in use.

7. Personal data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

A personal data breach shall be handled in accordance with the incident management plan and recorded in the personal data breach register.

If it occurs, the MFA is under an obligation to notify the competent supervisory authority, when possible within 72 hours after having become aware of it.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the MFA shall communicate it without undue delay to the data subject.

It is also the duty of all employees, officials and managers to immediately report any personal data breach of which they become aware to the Data Protection Officer (DPO).

All employees, officials and managers are liable to disciplinary action for the unlawful breach or transmission of personal data processed by the MFA, without prejudice to civil and criminal liability.

8. Professional secrecy

All employees, officials and managers of the MFA who handle personal data as part of their duties are obliged to keep personal data confidential and not to reveal or use them except in cases where the law requires them to do so.

The obligation of confidentiality shall remain in force, even after termination of duties, for as long as necessary to comply with the law.

It is expressly forbidden to use, make available or allow access by any means, even temporarily, to personal data by unauthorised personnel or those who do not need them for a defined purpose and in the exercise of the functions assigned.

9. Information and Training

All employees, officials and managers of the MFA are duly informed about the measures to be taken when processing personal data by the MFA and about the risks and consequences of unlawful processing.

The MFA's mission is to provide its employees with appropriate training and to keep them constantly updated on the measures to be adopted within the organisation.

For employees with regular access to personal data, the MFA is required to provide periodic awareness and IT security sessions.

10. Clarifications and filling of gaps

Requests for clarification of doubts in the interpretation or application of this Code of Conduct should be addressed to the Data Protection Officer, through the address epd@mne.pt, who will respond or forward to the corresponding department to be answered.

The provisions of the General Data Protection Regulation shall apply to any omissions in this Policy, as well as the national legislation in force on this matter.