Privacy Policy

(GDPR)

Table of contents

The Ministry of Foreign Affairs (MFA) values the privacy and protection of personal data, having practices and instruments in the field of security and protection of personal data, which meet the requirements established in the General Data Protection Regulation (GDPR), in force since 24 May 2016.

Therefore, the MFA has found it fitting to define the Privacy Policy in accordance with this manual.

1. Concept of personal data

Personal data is the information relating to an identified or identifiable natural person (data subject).

For this purpose, "identifiable" means that a natural person can be identified, directly or indirectly, in particular by reference to an identifier, such as: a name, an identification number, location data, identifiers by electronic means or by one or more specific elements related to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR, predicts certain categories of sensible data which cannot be processed except in exceptional cases, such as trade union membership, political opinions, religious or philosophical beliefs, biometric data, and health-related data

2. Objective

This document's objective is to define the MFA's Privacy Policy, as a set of principles and guidelines that must be considered during the execution of all processes involving the processing of personal data, as well as in the definition of the Security Policy, Code of Conduct and Privacy Statements.

In the MFA's Privacy Management System, the Privacy Policy is a fundamental document that constitutes an input to the main information security processes, communication with data subjects and third-party management.

It is a document that must be accessible internally at the MFA, but that can also be consulted by external data subjects, as complementary information referred to in the Privacy Statements, which are specified at each point of collection of personal data.

3. Scope

The Privacy Policy is applicable to the entire MFA organisation, including its External Network.

4. Privacy Principles

The MFA processes personal data in accordance with the principles determined in the article 5 of the GDPR.

Thus, the processing of personal data complies with the established principles:

a) Data processing is lawful, fair, and transparent in relation to the data subject;
b) Data are collected for specific, explicit, and legitimate purposes and shall not be further processed in a way that is incompatible with those purposes;
c) Only data that is adequate, relevant and limited to what is necessary for the purposes for which it is collected shall be collected;
d) The data collected must be accurate and updated whenever necessary, and all appropriate measures must be adopted to ensure that inaccurate data are erased and rectified without delay;
e) The data must be preserved in a way that allows the identification of the data subjects only for the necessary period, for the purposes for which they are needed;
f) The data must be processed in a way that ensures security, including protection against their unauthorised or unlawful processing and against accidental loss,

destruction or damage, by adopting appropriate technical and organisational measures;

g) The controller is accountable for and must be able to demonstrate compliance with the data processing regulation.

5. Lawfulness of processing

As the controller, MFA can only process data when at least one of the following conditions is met:

1) The data subject has given consent for one or more specific purposes;
2) It is necessary for the fulfilment of a legal obligation to which the MFA is subject to;
3) It is necessary for the protection of the vital interests of the data subject's or of another natural person;
4) It is necessary for the performance of tasks carried out in the public interest;
5) It is necessary for the legitimate interests pursued by the MFA, provided that the data subject's fundamental rights and freedoms, which require the protection of personal data, are ensured, especially if the data subject is a child.

To be considered valid, any consent request must be presented in an intelligible and prominent manner, in clear and simple language. Consent must be informed, which means that the data subject must receive adequate information regarding the data and the processing that will take place.

6. Data subjects' rights

Information or communications related to the processing of personal data must be easily accessible and understandable, and formulated in clear, simple, and concise language, in obedience to the principle of transparency.

The MFA commits to informing the data subjects about all relevant aspects regarding the processing of personal data such as:

- The identity and contact of the data controller;
- Contact details of the Data Protection Officer;
- Purpose and legal base for processing;
- The recipients of personal data, and if international transferences exist
- Data retention period;
- The rights of data subjects.

The MFA commits to respect the rights of data subjects, namely those set out in articles 17 and 18 of the GDPR:

a) The right of access – The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are subject to processing and, if so, the right to access his or her personal data and information concerning the purposes of processing, categories of personal data, recipients, retention period and existence of automated decisions;
b) The right of rectification- The data subject has the right to obtain, without undue delay, from the controller the rectification of inaccurate personal data;
c) The right to erasure - The data subject has the right to obtain from the controller the deletion of their personal data, when one of the following reasons applies: the personal data is no longer necessary for the original purpose, or consent has been withdrawn, or the data subject has exercised their right to object, or the data was processed unlawfully;
d) The right to restriction of processing- The data subject has the right to obtain from the controller the restriction of processing, if they contest the accuracy of the data or if the processing is unlawful;
e) The right to data portability- The data subject has the right to receive the personal data concerning them, which they have provided to a controller in a structured, commonly used, machine-readable format

f) The right to object- The data subject has the right to oppose at any given time, for personal reasons the processing of any data concerning them.

7. MFA's responsibility as controller

Considering the nature, scope, context, and purposes of data processing, as well as the risks to the rights and freedoms of natural persons, the probability and severity of which may vary, the MFA applies the adequate technical and organisational measures to ensure and to be able to demonstrate the lawful processing of data, in accordance with this regulation. These measures are reviewed and updated as necessary.

Data protection by design and by default- The MFA applies, both when defining the means of processing and during processing, the appropriate technical and organisational measures, aimed at effectively applying the principles of data protection and include the necessary safeguards in the processing, in a way which complies with the requirements of the GDPR and protects the data subjects' rights.

Equally, the MFA applies technical and organisational measures to ensure that only personal data that are necessary for each specific purpose of processing are processed and are not made available, without human intervention, to an indefinite number of natural persons. These measures are applied by default, that is, under any circumstances and even if no specification to that effect is available.

Records of processing activity- The MFA keeps a record of all processing activities under its responsibility. This record contains all the following information:

- The name and contact details of the controller and, where applicable, any joint controller, the controller's representative, and the data protection officer;
- The purposes of the processing;
- The description of the categories of data subjects and personal data

- The categories of recipients to whom personal data have been or will be disclosed, including recipients established in third countries or international organisations;
- If applicable, transfers of personal data to third countries or international organisations, including the identification of such third countries or international organisations;
- If possible, the predicted deadlines for the deletion of the different categories of data;
- If possible, a general description of the technical and organisational measures in the field of security.

Security of processing- The MFA applies the suitable 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 field, are detailed in the Security Policy.

Breach of personal data - In the event of a breach of personal data, the MFA notifies the National Data Protection Commission of the fact, whenever possible within 72 hours of becoming aware of such breach, and the data subject, without undue delay. When the breach of personal data is likely to entail a high risk for the rights and freedoms of individuals, the MFA informs the data subjects of the personal data breach.

Contents of the notice:

- Name and contact details of the data protection officer or other contact point where further information can be obtained;
- The presumable consequences of a personal data breach;
- The measures adopted or proposed by the MFA to remedy the breach of personal data, including measures to mitigate its possible negative effects, when appropriate.

In case of notification to the supervisory authority, it must contain a description of the nature of the personal data breach, including, if possible, the categories and approximate number of data subjects affected and the approximate number of personal data records concerned.

8. Data Protection Officer

The MFA has a Data Protection Officer (DPO) who:

- Monitors compliance of data processing with applicable standards;
- Provides information and advice, when requested, on their obligations, and issues regarding the processing and protection of personal data;
- It is the point of contact for the supervisory authority (National Data Protection Commission – NDPC) on issues related to the processing, cooperating with this entity.

Data subjects may contact the data protection officer on all matters related to the processing of their personal data and the exercise of the rights conferred on them by this regulation.

The data protection officer is bound by an obligation of secrecy or confidentiality in the exercise of their duties, in accordance with Union or Member State law.

9. Transfers of personal data to third countries or international organizations

Where data are transferred to a joint controller or processor of the MFA, located in a third country outside the European Union, a level of data protection equivalent to the protection afforded by the legislation in force in the EU, in particular as provided for in the GDPR, shall be maintained.

In the context of international data transfers, the MFA will follow one of the following procedures:

- Individual contract or standard contractual clauses adopted directly by the European Commission, or by a supervisory authority;
- Participation of the processor in an EU accredited or recognised certification system or standard, to ensure an adequate level of protection;
- Acknowledgement that the processor's binding corporate rules ensure an adequate level of data protection, issued by the supervisory authorities;
- Existence of an adequacy decision concerning the third country, the territory or specific sector of such third country, or concerning the international organisation in question.

The rules for carrying out cross-border data transfers will not always apply when there are occasional and necessary operations for the fulfilment of a contract or in the context of litigation (judicial, administrative, or with regulatory bodies or similar).

10. Institutional Relationships

Relationship between the MFA and processors in data transfers

Where processing is to be carried out on behalf of a controller, the MFA shall only subcontract credible, responsible entities that fully comply with the Regulation, through the signature of subcontracting contracts, that comply with the existing models in the MFA, where the processor ensures that it provides sufficient guarantees for the execution of adequate technical and organisational measures that are compliant with the requirements of the Regulation.

In the selection and definition of the terms of the relationships to be established with all its processors, the MFA shall endeavour to ensure that processors use the best technical and technological solutions appropriate to their reality with regard to personal data processing and information security.

The transmission of personal data to processors will only be carried out within the scope of contractually established relationships with the MFA and only when there is a justifiable basis for doing so.

Relationship between the MFA and joint controllers in the transmission of personal data

The MFA maintains, along with the joint controllers, the responsibility for the treatment of personal data in a fair, lawful and transparent manner.

The joint controllers collectively determine the purposes and means of the processing of personal data.

In agreement with each other and in a transparent manner, they must define their common responsibilities for compliance with the GDPR in the MFA, specifically regarding the exercise of the data subject's rights and the respective duties to provide the information stated in the regulation terms (duty to inform).

The essence of the agreement between the joint controllers must be made known to the data subject.

Institutional relationship with the National Data Protection Commission

The MFA has a duty to collaborate with the National Data Protection Commission, providing it with the necessary information, when requested.

The data protection officer will represent the MFA before the NDPC.

11. Clarifications and gap filling

Requests for clarification of any doubts in the interpretation or application of this Privacy Policy must be addressed to the Data Protection Officer, who will respond or forward them to the competent department for that purpose.

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