@EDMIS IRIDA
6684f301972ec454ab5e8800
Ref. No: Υ.Σ.4496
Signature: 03/07/24 10:15
Distribution: 03/07/2024 10:17

# Privacy Policy for the Processing of Biometric Data

**1. Purpose of this policy**

For the safety and security of the residents in the Accommodation Facilities of the Reception and Identification Service, the staff and visitors, the buildings and assets, the Ministry of Migration and Asylum (MMA) operates an access control system (entry – exit through a security turnstile, upon presentation of an individual card and simultaneous use of a fingerprint). This policy describes the operation of this system and the safeguards that the Ministry, as an organisation, takes in order to fulfil its data protection obligations in relation to the processing of Biometric Data and to protect privacy and other fundamental rights and legitimate interests. The MMA has taken care of the appropriate 'assurance' tools, such as certifications and marks, standard DPIAs, standard contracts.

1.1. The purpose of this Privacy Policy for the Processing of Biometric Data by the MMA ('the Policy') is to ensure that the processing of biometric data by the Hyperion system is carried out in accordance with the legislation on the protection of personal data. It also seeks to ensure that it is carried out in a way that takes into account the specific characteristics of biometric data, as well as the opportunities and risks associated with their processing.

1.2. The application of data protection rules in humanitarian action is imperative to safeguard the rights and dignity of individuals, to support the implementation of the principle of accountability and transparency of organisations processing personal data. For the MMA, the protection of personal data, the disclosure of which could put the data subjects at risk or which could otherwise be used for purposes other than those for which they were collected, is an integral means of preserving its neutrality, impartiality and independence, as well as the exclusively humanitarian nature of the mission of the MMA.

1.3. The MMA recognises that the responsible application of new technologies, including biometric identification techniques, can enhance the capability of its operations and the achievement of specific objectives based on the mandates it receives.

1.4. Biometric data are categorised as sensitive personal data in a growing number of jurisdictions and, consequently, their processing, as part of these legal regimes, is subject to specific legal restrictions and, in some cases, prohibited. Although the MMA processes personal data in accordance with its mission, increased protection of personal data whose disclosure could cause harm to individuals is required. These principles require humanitarian agencies to assess threats

to persons who provide them with information and to take the necessary measures to avoid negative consequences for those persons. Therefore, if the data are too sensitive and could cause Data Subjects harm that cannot be mitigated, then the data should not be collected in the first place. The MMA has established this Policy in recognition of the strong concerns related to the processing of biometric data. More specifically, the Policy limits the use of biometric data to specific situations and use methods, requires that Data Protection Impact Assessments be conducted before any new project or programme involving biometric data, adopts a data protection approach by design and by default for all biometric systems, to be transparent about its use of biometric data and to ensure that the rights of Data Subjects are preserved each time the data in question are processed.

1.5. Due to the rapid changes in technology and evolving data protection rules in this area, this Policy also binds the MMA to regularly review their application to ensure that the processing of biometric data does not inadvertently endanger the rights or safety of Data Subjects. This includes possible developments in the capabilities of specific biometric identification or analysis techniques, as well as changing attitudes and approaches regarding the use of biometric data by States, humanitarian and other non-state actors. It also aims to ensure that any new privacy-enhancing technologies that may be developed over time can be adopted, enabling the increased use of biometrics use cases, if required.

1.6. This Policy establishes:

(i) the roles and responsibilities of the staff and programmes of the MMA;
(ii) the Legal Basis for the processing of biometric data by the MMA;
(iii) the specified purposes and use cases in accordance with these legal bases;
(iv) the approved biometric data types and the approved processing techniques;
(v) the impact assessment on data protection and data protection requirements by design and by default;
(vi) the conditions that must be met in order to entrust the collection or processing of biometric data to third parties on behalf of the MMA;
(vii) the conditions and restrictions on data transmissions, including requests for access to governments, law enforcement authorities and judicial authorities; and
(viii) measures to ensure respect for the rights of Data Subjects, including transparency requirements.

**2. Scope of application**

2.1. The Policy applies to all biometric data processed by the staff and Information Systems (IS) of the MMA in accordance with their official tasks and activities, as well as to personal data processed by the MMA for the purpose of creating a biometric ‘standard‘ or ‘profile‘ regardless of its form. It therefore includes biological reference samples, images used for digital matching and the ‘transformed‘ data generated for comparison purposes.

2.2. The Policy also applies to staff authorised to process biometric data on behalf of the MMA by the Responsible Staff of each IS of the MMA, as applicable on a case-by-case basis.

2.3. The key elements of the Policy also apply to cases where the MMA may use biometric data for the purpose of verifying or authenticating the identity of its beneficiaries, or for the introduction and use of a fingerprint-based employee entry/exit control system, which constitutes a form of biometric-based employee screening. Biometric systems are applications of biometric technology aiming at the automatic identification and/or authentication of a natural person. The collection of biometric data (in this case, the fingerprint image) occurs during the process of registering the individual in the system. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person (Recital 51 of the GDPR).

2.4. The MMA, with respect to personal data, complies with the General Data Protection Regulation and the applicable national legislation as part of its activity and purpose and takes the envisaged and available technical and organisational measures as provided for in the General Data Protection Regulation and the Greek legislation by extension. As of 29-08-2019, Law 4624/2019 (Gov. Gaz. 137, Vol. A) applies adapted to and harmonised with the General Data Protection Regulation (EU 2016/679) of 25.5.2018 and the Directive (EU 2016/680) of the European Parliament, which strengthens the framework for the protection of data subjects with regard to the processing of personal data in the European Union. For the text of the Regulation you can select the URL: https://eurlex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679.

**3. Definitions**

3.1. '**Anonymisation'** means the transformation of personal data into anonymised data so that it is no longer possible to identify the individuals to whom the data relate. Data are not anonymised if this process can be reversed, either by decoding or through techniques, such as data matching, which allow re-identification.

3.2. '**Biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.

3.3. '**Data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.4. '**Controller'** means the natural or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

3.5. **'Data Protection Impact Assessment'** means the exercise to identify, assess and address risks to Personal Data arising from a project, policy, programme or other initiative implemented by the MMA.

3.6. '**Data Subject'** means a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.

3.7. '**Personal Data'** means any information relating to an identified or identifiable natural person. Such data may be an identifier, such as a name or audiovisual material, an identification number, location data, or an online identifier. It may also mean information related specifically to the physical, physiological, genetic, mental, economic, cultural or social identity of a Data Subject. The term also includes data that identify or can identify human remains.

3.8. **'Pseudonymisation'** means the replacement of personal identifiers, such as a person's name, with a unique identifier that is not linked to their "real world" identity using techniques such as encryption or hashing.

3.9. '**Responsible Staff'** means the member of the authorised staff of the MMA in each sectoral structure or in the Central Service, who is entrusted with the management of a specific area of activity or a specific IS (e.g. Unified IS for Reception and Asylum (HYPERION - ALKYONI II), Centaur) as part of the mandate received by the MMA. The Responsible Staff includes the programme coordinator, or staff members authorised by them to act as Responsible Staff of the MMA.

**4. Roles and responsibilities**

4.1. The MMA is the Controller of biometric data and related Personal Data processed thereby in accordance with the Personal Data Protection legislation, as defined in this Policy, when determining the purpose and means for which such data may be used, including when such data may be disclosed to partners.

4.2. The MMA is responsible for approving new processing, periodically reviewing this Policy and adopting any changes.

**5. Legal basis for processing biometric data**

5.1. Pursuant to the Personal Data Protection legislation, the legal basis for the processing of biometric data for the specific purposes set out in Article 6 GDPR, i.e. the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, while the processing of special categories of (biometric) data (fingerprint) takes place for reasons of substantial public interest (Article 9 (2)(g) GDPR) under the Dublin III Regulation or the Immigration Code, while the Closed Controlled Access Centres (CCAC) constitute 'critical infrastructures of the State.'

(i) the 'important public interest reasons' for the use of biometric data linked to an order for the identification of individuals for the purpose of providing specific humanitarian services and other humanitarian emergencies. (ii) the 'legitimate interest' of using biometric data for:

(a) the strict protection of confidential information and resources critical to the mission of the MMA;

(b) the provision to beneficiaries of humanitarian services of a token-based verification credential that can be used to verify receipt of such services, when the token is in the possession of the Data Subject and the MMA does not maintain a database of biometric data.

There is no processing of personal data by the Hyperion and Centaur programmes in order to extract special categories of personal data (e.g. political opinions from video images showing persons who have taken part in protests), and therefore Article 9 GDPR does not apply in principle.

**6. Specific purposes of biometric data processing**

6.1. The MMA processes biometric data for specific humanitarian purposes and may only use it for these purposes.

6.2. Following an extensive review of biometric data processing operations, the following use cases have been approved by the MMA for these specific humanitarian purposes:

(i) the use of biometric identification systems to screen incoming and outgoing persons or to restrict access to guarded areas and facilities of the MMA, where the processing of such data is limited to specific internal areas requiring a high level of security and to staff authorised to enter them;

(ii) the use of biometric data for identification purposes;

(iii) the inclusion of fingerprints to provide beneficiaries of humanitarian services and assistance with a token-based verification credential, such as a card that can be used to verify receipt of such services, when the token is kept on a medium held by the Data Subject and the MMA does not maintain a biometric database.

**7. Adequacy, relevance and minimisation of biometric data**

7.1. According to the Personal Data Protection legislation, data processed for a specified purpose must be relevant and not exceeding what is required in relation to the specific purposes. According to this requirement, where the MMA intends to process biometric data, it must first document that the intended purpose and the requested results of the processing could not have been achieved without the use of biometric data.

7.2. Pursuant to the principles of data adequacy, data relevance and the destruction of data that are no longer needed, the MMA should ensure that biometric data and additional personal data related to them are processed to the minimum extent possible. In practice, this means collecting only the data that are strictly necessary to achieve the intended purpose(s), erasing biometric data as soon as they are no longer necessary,

restricting access to the data in accordance with the 'need-to-know' principle and any other safeguards, and not disclosing biometric data unless such transmissions meet the conditions set forth by law.

**8. Non-mandatory nature of biometric processing**

8.1. Although certain humanitarian services provided by the MMA for the implementation of the objectives based on the mission it has undertaken to carry out may not be possible without the processing of biometric data, the MMA will not make the provision of biometric data a mandatory condition for the provision of the service.

**9. Data protection impact assessment for processing operations involving biometric data**

9.1. For approved use cases and processing techniques, a Data Protection Impact Assessment must be carried out by the relevant programme or agency prior to the creation of any new project or programme that includes biometric data. Where a DPIA has already been carried out to address risks relating to data protection and information security for a similar project or programme which is considered applicable to the envisaged processing, no further DPIA is required.

9.2. When conducting the Data Protection Impact Assessment, the MMA must assess the risk that the MMA, or any partners or service providers involved in the processing, may not be able to refuse requests for access to data from the authorities. That assessment must be subject to regular review.

9.3. A Data Protection Impact Assessment must also be carried out by the MMA before the organisation uses biometric data collected by other humanitarian organisations to verify or authenticate the identity of recipients of the humanitarian services by the MMA.

9.4. A Data Protection Impact Assessment must also be carried out before biometric data is transferred to a governmental body or authority for humanitarian purposes.

9.5. A copy of the Data Protection Impact Assessment carried out for biometric data must be available to the Data Protection Officer of the MMA and the Hellenic DPA.

9.6. New processing techniques require consultation with the Data Protection Officer prior to the commencement of the Data Protection Impact Assessment, who can provide guidance as to its focus and content, the mitigation measures that must be taken and the means of implementation.

**10. Data protection by design and by default and security of biometric data processing**

10.1. The MMA must ensure that new systems, programmes and projects processing biometric data are developed by design and by default in accordance with the principle of data protection. This requires the implementation of high level data security features, as well as technical and organisational measures to ensure

that the requirements of this policy are met by design and by default. Data protection by design and by default also requires the adoption of the least intrusive and least risky form of processing as set out in **Annex 1**.

10.2. Any existing systems for controlling authorised entry-exit do not include by design the processing of biometric data and were created before the adoption of this Policy. In any case, all existing procedures and systems for controlled entry and exit will be reviewed.

10.3. Taking into account the operational needs of the biometric system, the MMA must develop or implement the following security features:

(i) biometric data are protected by state-of-the-art data security measures, including encryption of data at rest and in transit, to minimise the risk of unauthorised access;

(ii) systems are designed to prevent unauthorised disclosure of biometric data using technical means, including the "one-way coding" of biometric images and the use of recognised algorithms for the conversion and matching of biometric patterns;

(iii) despite the need to maintain a link between these datasets, database snapshots are separated, and biometric data records are stored separately from the personal data with which they are associated;

(iv) audit trails are established for the use of all biometric data processed by the MMA.

10.4. When designing biometric systems and taking into account the functional needs of the biometric system, the MMA must ensure that:

(i) a beneficiary-centred (or user-centred) approach regarding data ownership is built into the system architecture and the related policies, ensuring that the Data Subject is aware of the processing, can access his or her data, understands how they have been used and makes decisions about their continued processing;

(ii) the principle of data minimisation is effectively applied to the processing of personal data linked to a biometric profile, such processing being strictly limited to the information necessary to achieve the specified purpose; and

(iii) pseudonymisation techniques are applied to the processing of personal data associated with the biometric data.

10.5. When implementing biometric systems, the MMA must ensure that:

(i) the Framework of Accountability to Data Subjects and where possible participation in the programmatic planning, risk assessment and mitigation process;

(ii) that access to biometric data by the MMA staff and third party service providers is as limited as possible;

(iii) that standard operating procedures are followed to ensure that all personal data are accurate and up to date and that every reasonable precaution is taken to ensure that inaccurate data are rectified or erased without undue delay;

(iv) that the technical and organisational measures and their supervision prevent any further processing of biometric data for purposes other than the specified purpose for which they were collected.

**11. Use of biometric data collected by third parties to verify the identity of recipients of humanitarian services provided by the MMA.**

11.1. The MMA, through the Unified IS for Reception and Asylum (HYPERION - ALKYONI II), derives simple personal data (identification data) of applicants for international protection from the Alien Traffic Mapping system of the Hellenic Police, through an interoperable call over https, between the central servers of the two institutions. The information is drawn from the Unified IS for Reception and Asylum (YPERION - ALKYONI II), which is used exclusively by the Services of the MMA responsible for International Protection.

**12. Authorities' requests for access to biometric data**

12.1. The MMA is aware of the value of biometric data in the tracking and identification of persons of concern to States and security bodies, law enforcement and judicial authorities, and understands that these authorities are particularly interested in obtaining such data. This interest may extend to the use of biometric data for purposes which, although in some cases perfectly legitimate on the part of the authorities, may not be compatible with the neutrality, impartiality and independence of the MMA, as well as with the exclusively humanitarian nature of the MMA's work and the vital interest of the Data Subject. These purposes could include border and immigration control, counter-terrorism and national security.

12.2. In order to safeguard the neutrality, impartiality and independence of the MMA, as well as the exclusively humanitarian nature of its work, the MMA will not disclose or otherwise transfer biometric data to any government or authority unless all of the following conditions are met:

(i) the transfer is in the vital interest of the data subject or another person;
(ii) the transfer is necessary to enable an authority to fulfil a humanitarian obligation;
(iii) the Data Subject has been informed that the transfer of the data is envisaged and does not object;
(iv) a Data Protection Impact Assessment (DPIA) has been completed prior to the disclosure of the data and the DPIA has not identified risks to data subjects or other persons that outweigh the perceived benefits of the disclosure.
(v) The recipient undertakes in writing to use the transferred data only for the specified humanitarian purpose.

12.3. When the Responsible Staff receives a request from an authority and believes that there may be difficulties in the MMA's compliance with the above requirements, the MMA's Data Protection Officer must be informed immediately and, if necessary, forward the matter to the Directorate for a decision to be taken.

**13. Retention of biometric data**

13.1. All biometric data should be subject to a retention period that is explicitly linked to the specific purpose for which they were collected. Biometric data may be retained by the MMA only for as long as necessary for that specific purpose.

13.2. If at the end of the retention period it is determined that the biometric data are no longer necessary, then the data should be deleted. If at the end of the retention period it is established that the biometric data are still necessary for the MMA for the humanitarian purpose in question or for a compatible humanitarian purpose, the retention period may be renewed or extended.

13.3. No archiving of biometric data is allowed by the MMA, unless the Data Subjects have consented thereto.

**14. Rights of the Data Subjects**

14.1. The MMA, in full compliance with the provisions of the GDPR, satisfies and facilitates the exercise of the rights of the Subjects provided for in the GDPR, provided that it is possible to exercise them effectively, namely:

14.2. The right of access in order to inform the data subjects which data are processed by the Ministry of Digital Governance, for what purpose and their recipients.

14.3. The right to rectification in order to correct errors, inaccuracies and omissions in the data of the data subjects.

14.4. The right to erase them in order, under the conditions of the GDPR, to erase the data of the subjects from the files of the MMA.

14.5. The right to restrict processing in the event that the accuracy of the data is contested, where the right to object has been exercised and the decision is pending and where the data are no longer necessary for the original purpose but for legal reasons cannot yet be erased.

14.6. The right to portability in order for the data of the subjects to be received in electronic format.

14.7. The right to object to the processing of personal data by withdrawing the subject's consent, if consent was required, without such withdrawal affecting the lawfulness of the processing for the period of time preceding the withdrawal of consent.

14.8. Where the data subject objects to the provision of biometric data, the MMA must provide the humanitarian services to the Data Subject without processing his or her biometric data.

**15. Fulfilment of rights – Safeguards – Retention Period**

Overall, the MMA ensures that:

Procedures are in place allowing the rights of Data Subjects to be easily exercised so that all required actions can be initiated immediately.

It will respond to a request submitted by a data subject without undue delay and in any case not later than thirty (30) calendar days. Where it cannot satisfy a right exercised by the Data Subject, the MMA shall ensure that a specific, adequate and complete justification is provided.

Except in cases of manifestly unfounded or excessive requests, all actions concerning the satisfaction of the rights of the Data Subjects will be carried out free of charge for the Data Subjects.

The personal data collected are recorded in computerised systems, which provide adequate security and are used by specially trained and authorised employees, in order to achieve the maximum possible protection of the data recorded in the modern digital environment.

The MMA retains and processes personal data for the purposes mentioned above only for as long as necessary for the purpose for which they were collected or in accordance with the applicable legislation.

In the event of the exercise of one of the aforementioned rights, the MMA will take all possible measures to satisfy it within thirty (30) calendar days of receipt of the request, informing in writing whether it is satisfied, or the reasons that prevent the exercise. If, due to the complexity or the number of requests, this is not technically possible, the time limit will be extended for another two months after informing you.

If you are not satisfied with the response or if you consider that the processing of your Personal Data violates the applicable regulatory framework for the protection of personal data, you have the right to submit a complaint to the Hellenic Data Protection Authority (postal address: 1-3 Kifisias Avenue, P.C. 115 23, Athens, tel. (+30) 2106475600, e-mail contact@dpa.gr).