PERSONAL DATA PROTECTION POLICY

1. Subject-matter of the Personal Data Protection Policy

a. The Hellenic Ministry of National Defence (henceforth HMoND), located at Camp Papagou, 229-231 Mesogion Avenue, GR-15561, Holargos, Attica, Greece, respects the privacy and personal data of data subjects and takes care to comply and demonstrate compliance with the General Data Protection Regulation (EU) 2016/679 (henceforth GDPR), Implementing Law 4624/2019 (GG A 137), and all provisions of national and Union law on personal data protection.

b. With this Personal Data Protection Policy, the HMoND, as controller, informs natural persons (data subjects) on the collection and processing of their personal data, the protection of such data, their relevant rights, and methods for contacting the Ministry.

2. Definitions

- **"Personal data":** any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person [Article 4 (1) GDPR].

- **"Special categories of personal data" (former sensitive):** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation [Article 9 (1) GDPR].

- **“Processing”:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction [Article 4 (2) GDPR].

- **“Restriction of processing”:** the marking of stored personal data with the aim of limiting their processing in the future [Article 4 (3) GDPR].

- **“Profiling”:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements [Article 4 (4) GDPR].

- **“Pseudonymisation”:** the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [Article 4 (5) GDPR].

- **“Encryption”:** The process in which personal data are converted into an unintelligible format using algorithms and encryption keys. The encrypted data can only be read by authorised users holding the encryption keys.

- **“Anonymisation”:** the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject.

- **“Controller”:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law [Article 4 (7) GDPR].

- **“Processor”:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller [Article 4 (8) GDPR].

- **“Recipient”:** a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing [Article 4 (9) GDPR].

- **“Third party”:** a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data [Article 4 (10) GDPR].

- **“Consent of the data subject”:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [Article 4 (11) GDPR].

- **“Personal data breach”:** 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 [Article 4 (12) GDPR].

- **“Genetic data”:** personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question [Article 4 (13) GDPR].

- **“Biometric data”:** 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, such as facial images or dactyloscopic data [Article 4 (14) GDPR].

- **“Data concerning health”:** personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status [Article 4 (15) GDPR].

- **“Supervisory authority concerned”:** The Hellenic Data Protection Authority (henceforth DPA) (Article 4 par. C of L. 4624/2019).

3. Principles relating to processing of personal data

The HMoND respects the principles relating to processing of personal data.

a. Principle of lawfulness, fairness and transparency

The HMoND processes personal data lawfully, fairly and in a transparent manner in relation to the data subject (Article 5 par. 1 sec. a GDPR).

b. Principle of purpose limitation

The HMoND collects the personal data for specified, explicit and legitimate purposes and does not further process these in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (Article 5 par. 1 sec. b GDPR).

c. Principle of data minimisation

The HMoND takes appropriate technical and organisational measures in order for the personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Article 5 par. 1 sec. c GDPR).

d. Principle of data accuracy

The HMoND takes the necessary steps in order for the personal data to be accurate and, where necessary, kept up to date; every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (Article 5 par. 1 sec. d GDPR).

e. Principle of storage limitation

The HMoND keeps the personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, as specifically defined in applicable legislation and in the relevant Military Regulations and Orders. In exceptional cases, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (Article 5 par. 1 sec. e GDPR).

f. Principle of integrity and confidentiality

The HMoND ensures that the personal data are processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Article 5 par. 1 sec. f GDPR).

g. Principle of accountability

The HMoND shall be responsible for and take the measures deemed necessary in order to be able to demonstrate compliance with the above principles (Article 5 par. 2 GDPR).

4. Purposes of processing

The HMoND processes personal data in order to exercise its powers provided by law, comply with its legal obligations deriving from national and Union law, perform tasks carried out for the purposes of National Defence, in the public interest and in the exercise of official authority vested in it.

5. Lawfulness of processing

The HMoND ensures that the processing of personal data is lawful and undertakes to proceed with such processing exclusively and only if there is a legal basis that permits the processing, as follows:

a. The data subject has given consent to the processing of his or her personal data for one or more specific purposes (Article 6 par. 1 sec. a GDPR).

b. The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6 par. 1 sec. b GDPR).

c. The processing is necessary for compliance with a legal obligation to which the HMoND is subject (Article 6 par. 1 sec. c GDPR).

d. The processing is necessary in order to protect the vital interests of the data subject or of another natural person (Article 6 par. 1 sec. d GDPR).

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 HMoND (Article 6 par. 1 sec. e GDPR).

f. With regard to the processing of personal data carried out in the context of activities directly related to national defense and security, the provisions of the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data apply [Convention 108/1981 of the Council of Europe, ratified by Law 2068/1992 (A' 118)], in combination with the special provisions of Law 4624/2019.

6. Categories of data subjects and personal data

a. Categories of data subjects:

(1) Military and civilian personnel serving or working in the HMoND, respectively

(2) Civilians (**including, but not limited to:** contractors, visitors, suppliers, etc.)

b. Categories of personal data (**including, but not limited to, and where appropriate:** personal information, work data, financial information (e.g. IBAN), etc.

7. Special categories of personal data

The HMoND may process data which fall within special categories of personal data (former “sensitive”), such as data concerning health, only as provided by Articles 9 of GDPR and 22 of L. 4624/2019 (GG A 137).

8. The rights of the data subject

a. Data subjects have in summary the following rights against the HMoND with regard to the protection of their personal data, subject to the terms, conditions, restrictions, and exceptions of Articles 12 through 21 and 23 of GDPR and Articles 29 par. 2, 30 par. 2, and 31 through 35 of L. 4624/2019:

(1) **Right to information:** The data subject shall have the right to know the categories of personal data processed by the HMoND, as well as the purposes of processing.

(2) **Right of access:** The data subject shall have the right to obtain access to the personal data processed by the HMoND.

(3) **Right to rectification:** The data subject shall have the right to obtain the rectification of inaccurate personal data processed by the HMoND and to have incomplete personal data completed.

(4) **Right to erasure:** The data subject has the right to request from the HMoND the deletion of his/her personal data, under the conditions of applicable legislation and provided that there are no legal restrictions on the right.

(5) **Right to restriction of processing:** The data subject shall have the right to obtain from the HMoND restriction of his or her personal data processing as provided by applicable law.

(6) **Right to data portability:** The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the HMoND, as well as the right to transmit those data to another controller where the processing is based on consent or on a contract and is carried out by automated means.

(7) **Right to object:** The data subject shall have the right to object, as provided by applicable law, to processing of personal data concerning him or her on grounds relating to his or her particular situation.

b. The HMoND takes appropriate measures to facilitate data subjects to exercise their above rights, to respond to corresponding requests for information and to generally satisfy the above rights within the legal deadlines, taking into account restrictions for reasons of national defense, security or public interest.

9. General obligations of the controller

The HMoND implements and updates, if required, all appropriate technical and organisational measures and personal data protection policies to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR, taking into account the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons (Article 24 GDPR).

10. Security of personal data processing (Article 32 GDPR)

a. The HMoND shall implement appropriate technical and organisational measures to ensure a level of security for personal data processing appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

b. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

c. The HMoND shall take steps to ensure that any natural person acting under its authority who has access to personal data does not process them except on instructions from the HMoND, unless he or she is required to do so by Union or Member State law.

11. Personal data breach

a. The HMoND has appropriate procedures in place to manage a breach of security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

b. In the case of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, the HMoND must without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the personal data breach to the DPA. Where the notification to the DPA is not made within 72 hours, it shall be accompanied by reasons for the delay (Article 33 GDPR).

c. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the HMoND undertakes to communicate the personal data breach to the data subjects without undue delay, unless it has implemented appropriate technical and organisational protection measures or subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise (Article 34 GDPR).

12. Right to file a complaint with the Hellenic Data Protection Authority

Data subjects have the right to file a complaint with the Hellenic Data Protection Authority on matters related to processing of their personal data. Detailed information on how to file a complaint is provided on the Hellenic Data Protection Authority website (www.dpa.gr).

13. Visiting the General Directorate of National Defence Policy and International Relations website

a. The General Directorate of National Defence Policy and International Relations (GDNDPIR) website operates under the domain name: www.gdpeads.mod.mil.gr.

b. The GDNDPIR website operates as an information portal, providing the public with information on the GDNDPIR activities, relevant legislation, as well as access to services provided by the GDNDPIR (communication via e-mail).

c. For the use of the website and the effective and lawful provision of the aforementioned service, the HMoND processes the following personal data, which are retained for a period of 30 days:

(1) IP address, which is assigned to the device which the “user” uses to connect to the “service”.

(2) Timestamp of the “service”.

(3) Connection device information (operating system, browser).

d. The HMoND does not collect or process special categories of personal data for the purposes of providing the “service”. It may, however, process special categories of data if such data are input by the user when sending an e-mail message to the GDNDPIR e-mail address (gdpeads_gram@mod.mil.gr), which is posted on the website.

e. The personal data collected by the website and stored in a relevant database, are not subject to automated decision-making processes or “user profiling” and processed for the following purposes:

(1) to fulfil the purpose of the website, i.e. to provide information to users on GDNDPIR activities,

(2) to keep the website and the “service” running without interruption,

(3) to provide easy and user-friendly use of the website and

(4) to improve the web experience during operation of the “service”.

f. The website uses the UserWay website accessibility tool, which provides accessibility enhancement features for visitors (e.g. font size adjustment, color contrast, etc.). This tool is used solely for accessibility purposes and is not used for user behavior analysis, advertising targeting, or tracking purposes. During its use, necessary cookies may be activated, which are essential for the proper functioning of the accessibility services and do not require consent, in accordance with applicable legislation. These cookies are not used for tracking, behavior

analysis, or advertising targeting purposes. The operation of the tool is provided by a third-party provider (“UserWay Inc.”), which may process technical data (such as IP address) that are necessary for the provision of the service, in accordance with its own privacy policy, which is available at the electronic address “userway.org/privacy”.

14. Visitor/user responsibility

The visitor/user of the website must use the website's services in accordance with applicable legislation and refrain from any illegal, malicious or abusive action that may affect the security, availability and proper functioning of the HmoND information systems.

15. Conclusion

The HMoND acknowledges that personal data protection is a continuous process that requires constant monitoring and updates. To this end, it shall take make every effort to consolidate the concept of personal data protection and foster a relevant culture and awareness to all military and civilian personnel of the Armed Forces.

16. Contact

The HMoND has assigned a Data Protection Officer whom data subjects can contact via e-mail (e-mail: dpo@mod.mil.gr) or by phone at 210-6598205 for any information or assistance in exercising or understanding their rights and questions concerning their personal data, this Policy, and personal data protection in general.

17. Updates to the Personal Data Protection Policy

The HMoND may amend this Personal Data Protection Policy in order to comply with its legal obligations. The latest version of the Policy, can be found in the GDNDPIR website.

June 2026