Data Protection Policy Statement

1. Introduction

HPD, with registered address at 45, Grigoriou Lambraki St., Glyfada, Athens, Greece is committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information HPD collects and processes in accordance with the EU General Data Protection Regulation.

1.1 Background to the General Data Protection Regulation ('GDPR')

The EU General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/ EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 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.

Data 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.

Data subject (individual) – any living individual who is the subject of personal data held by an organisation.

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.

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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Consent – 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 the data subject.

Child – anyone under the age of 16 years old, although this may be lowered up to 13 years old subject to Member State law. The processing of the personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

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.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Data Protection Policy statement

2.1. This policy describes the relevant policies held and followed by HPD, such as the Information Security Policy (ISP), in order to collect, handle and store personal data. HPD acknowledges the importance of compliance with the GDPR and the respect of individual's rights, and commits to comply with both the law and good practice.

2.2. The GDPR and this policy shall apply to all Employees/Staff/Contractors/Clients/Partners and third party providers of HPD, to all of HPD's data processing functions, and any other personal data the organisation processes from any source. The legal basis for data processing and temporary recording in HPD's files is based on art. 6 paragraph 1 point b of GDPR. Any breach of the GDPR will be dealt under HPD's Breach Notification Procedure and/or through the Incident Management Centre (IMC) and may consist of a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.3. HPD has appointed a Data Protection Officer (DPO), who shall be responsible for reviewing the register of data processing annually in the light of any changes to HPD's activities.

2.4. Partners and any third parties working with or for HPD, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by HPD without having first entered into a Data Confidentiality Agreement, which imposes on the third-party obligations no less onerous than those to which HPD is committed, and which gives HPD the right to audit compliance with the agreement.

3. Responsibilities and roles under the GDPR

3.1. HPD is a data controller for staff and marketing data and a data processor for client data under the GDPR. HPD holds and follows a Training Policy which sets out specific GDPR training and awareness requirements in relation to specific roles and Employees/Staff of HPD generally.

3.2. The DPO and all those in managerial or supervisory roles throughout HPD are responsible for developing and encouraging good information handling practices within HPD. The DPO's role is specified in the GDPR. The DPO is accountable to Board of Directors of HPD for the management of personal data within HPD and for ensuring that HPD is in compliance with data protection legislation and good practice. This accountability includes development and implementation of the GDPR as required by this policy, and security and risk management in relation to compliance with the policy. The DPO shall have specific responsibilities in respect of procedures such as the Subject Access Request Form and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

3.3. Compliance with data protection legislation is the responsibility of all Employees/Staff of HPD who process personal data. They are also responsible for ensuring that any personal data about them and supplied by them to HPD is accurate and up-to-date.

4. Information Security Policy (ISP)

HPD takes the security and privacy of the data subjects and their personal data very seriously and undertakes every reasonable precautions and measures to secure and protect personal data that processes. To support compliance with the GDPR, HPD Board has approved and supported the development, implementation, maintenance and continual improvement of an ISP.

In determining its scope for compliance with the GDPR, HPD considers:

- any external and internal issues that are relevant to the purpose of HPD and that affect its ability to achieve the intended outcomes of its ISP;
- specific needs and expectations of interested parties that are relevant to the implementation of the ISP;

- organizational objectives and obligations;
- the organisation' s acceptable levels of risk; and
- any applicable statutory, regulatory, or contractual obligations.

5. GDPR Principles

To ensure HPD's obligations under GDPR are met, we process personal in accordance with six fundamental principles. These are:

a. Personal data must be processed lawfully, fairly and transparently

Lawfully – you must identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example, consent (explained herein under no. 7).

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the DPO;
- thepurposesoftheprocessingforwhichthepersonaldataareintendedaswellasthelegalbasis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- any further information necessary to guarantee fair processing.

b. Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of HPD's GDPR register of processing. The Privacy Procedure sets out the relevant procedures.

c. Personal data must be processed only where it is adequate, relevant and limited to what is necessary for processing

The DPO is responsible for ensuring that HPD does not collect information that is not strictly necessary for the purpose for which it is obtained.

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or a link to privacy statement and approved by the DPO.

The DPO will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

d. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. The DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

Employees/Staff/clients/contractors and third-party providers should be required to notify HPD of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of HPD to ensure that any notification regarding change of circumstances is recorded and acted upon.

The DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On at least an annual basis, the DPO will review the retention dates of all the personal data processed by HPD, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Information Disposal Policy.

The DPO is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If HPD decides not to comply with the request, the DPO must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

e. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

Where personal data is retained beyond the processing date, it will be minimised/encrypted/pseudonymised in order to protect the identity of the data subject in the event of a data breach. Personal data will be retained in line with the ISP and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

The DPO must specifically approve any data retention that exceeds the retention periods defined in the ISP and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

f. Personal data must be processed in a manner that ensures the appropriate security

In determining appropriateness, the DPO should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on HPD itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the DPO will consider the following:
• Password Protection
• Automatic locking of idle terminals;
• Removal of access rights for USB and other memory media;
• Virus checking software and firewalls;
• Role-based access rights including those assigned to temporary staff;
• Encryption of devices that leave the organisations premises such as laptops;
• Security of local and wide area networks;
• Privacy enhancing technologies such as pseudonymisation and anonymisation;
• Identifying appropriate international security standards relevant to HPD.

When assessing appropriate organisational measures, the DPO will consider the following:
• The appropriate training levels throughout HPD;
• Measures that consider the reliability of employees (such as references etc.);
• The inclusion of data protection clause in employment contracts;
• Identification of disciplinary action measures for data breaches;
• Monitoring of staff for compliance with relevant security standards;

• Physical access controls to electronic and paper-based records;
• Adoption of a clear desk policy;
• Storing of paper-based data in lockable fire-proof cabinets;
• Restricting the use of portable electronic devices outside of the workplace;
• Restricting the use of employees' own personal devices being used in the workplace;
• Adopting clear rules about passwords;
• Making regular backups of personal data and storing the media off-site.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. HPD's compliance with this principle is contained in its ISP.

The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

HPD will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, breach notification procedures and incident response plans.

6. Rights of individuals

Each individual shall have the following rights regarding data processing, and the data that is recorded about them:

- To make access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

HPD ensures that individuals may exercise these rights by making data access requests as described in the Acceptable Use Agreement, which shall include the Subject Access Request Form. This procedure also describes how HPD will ensure that its response to the data access request complies with the requirements of the GDPR.

Individuals shall also have the right to complain to HPD related to the processing of their personal data, handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

7. Consent

7.1. HPD understands “consent” to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject’s wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time. HPD understands “consent” to mean that the data subject has been fully informed of the in- tended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

7.2. There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The controller must be able to demonstrate that consent was obtained for the processing operation. For sensitive data, explicit written consent of individuals must be obtained unless an alternative legitimate basis for processing exists. In most instances, consent to process personal and sensitive data is obtained routinely by HPD using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

7.3. Where HPD provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16. HPD does not routinely process data in this category.

8. Security of Data

8.1. All Employees/Staff are responsible for ensuring that any personal data that HPD holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by HPD to receive that information and has entered into a confidentiality agreement.

8.2. All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy.

8.3. Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of HPD. All Employees/Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

8.4. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the Information Disposal Policy.

9. Disclosure of Data

HPD must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of HPD’s business.

10. Retention and Disposal of Data

10.1. HPD shall not keep personal data in a form that permits identification of data subjects for longer than a period which is for HPD necessary, in relation to the purpose(s) for which the data was originally collected. HPD may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

10.2. The retention period for each category of personal data will be set out in the ISP along with the criteria used to determine this period including any statutory obligations HPD has to retain the data. Manual records that have reached their retention date are to be shredded and disposed of as "confidential waste". Hard drives of redundant PCs are to be removed and immediately destroyed as required by the Information Disposal Policy.

10.3. HPD's information retention and information disposal procedures apply in all cases. Personal data must be disposed of securely in accordance with the sixth principle of the GDPR. Any disposal of data will be done in accordance with the secure disposal procedure.

11. Data Transfers

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as "third countries") are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The broader area of the EEA is granted "adequacy" on the basis that all such countries are signatories to the GDPR. The non-EU EEA member countries (Liechtenstein, Norway and Iceland) apply EU regulations through a Joint Committee Decision.

Privacy Shield
Should HPD wish to transfer personal data to an organization in the Unites States, HPD should check whether the organization is signed up with the Privacy Shield framework at the U.S. Department of Commerce.

Binding corporate rules
HPD may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that HPD is seeking to rely upon.

Model contract clauses
HPD may adopt approved model contract clauses for the transfer of data outside of the EEA. If HPD adopts the model contract clauses approved by the relevant supervisory authority there is an automatic recognition of adequacy.

Exceptions
In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/ or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the individual has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the individual and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

12. Complaints and queries

HPD tries to meet the highest standards to fulfill its obligations for any personal data it may hold. We take any and all complaints very seriously. For any queries or complaints about your personal data, you may put a request in writing using the below address:

HPD Data Protection Officer
(dpo@hpdlaboratory.com or G. Lampraki 45 &Tataki St., Glyfada, 16675, Athens, Greece)