1. INTRODUCTION

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

The 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 (if applicable).

1.2 Definitions used by the organization (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

1.3 Definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative center. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

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.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of 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.

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 – any living individual who is the subject of personal data held by an organization.

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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyze or predict that person’s performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorized 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 data protection authority

and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means 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.

Data protection authority – means Hellenic Data Protection Authority, located at Kifissias 1-3, PC 115 23, Athens, Greece, Telephone: +30-210 6475600, E-mail: contact@dpa.gr

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of 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 authorized 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 authorized to process personal data.

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

2. POLICY STATEMENT

- This Policy applies to all UNIPAKHELLAS affiliated and sister companies in Greece for the purposes of GDPR and has been decided that the leading entity for GDPR purposes will be UNIPAKHELLAS which will make sure that this Policy is duly approved and implemented by the companies related to it, to the extend it is applied taking into consideration the nature and way of collection of Personal data. Wherever in this Policy, UNIPAKHELLAS is stated, any related entity for the purposes of GDPR, collecting and/or determining the purposes and means of the processing of Personal data, should be also included.

- The Board of Directors and management of the Company are 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 UNIPAKHELLAS collects and processes in accordance with the General Data Protection Regulation (GDPR)

- Compliance with the GDPR is described by this policy, other relevant policies and procedures that are referred to in this document.

- The GDPR and this policy apply to all of UNIPAKHELLAS personal data processing functions, including those performed on customers', customers', employees', suppliers' and partners' personal data, and any other personal data the organization processes from any source.

- The GDPR Owner/DPO is responsible for reviewing the record of processing activities in the light of any changes to UNIPAKHELLAS activities and to any additional requirements identified by means of data protection impact assessments and the Compliance Officer always monitors GDPR Owner/DPO.

- This policy applies to all Employees of UNIPAKHELLAS, customers and any outsourced suppliers. Any breach of the GDPR will be dealt with under UNIPAKHELLAS disciplinary rules, according to which the breach of the GDPR is a cause for termination of the respective agreement (employment, service etc) and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

- Partners, employees and any third parties working with or for UNIPAKHELLAS, 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 UNIPAKHELLAS without either having first entered into a data confidentiality agreement or having a service agreement which includes confidentiality provisions and GDPR compliance covenants which imposes on the third party obligations no less onerous than those to which UNIPAKHELLAS is committed, and which gives UNIPAKHELLAS the right to audit compliance with the agreement.

3. RESPONSIBILITIES AND ROLES UNDER THE GENERAL DATA PROTECTION REGULATION

3.1 Company Responsibilities

- UNIPAKHELLAS is a data controller under the GDPR and as also the affiliated and sister companies in Greece for the purposes of GDPR, making sure that any UNIPAKHELLAS entity which due to its activity is considered as a controller, complies with GDPR.
- Top Management and all those in managerial or supervisory roles throughout UNIPAKHELLAS are responsible for developing and encouraging good information handling practices within UNIPAKHELLAS; responsibilities are set out in individual job descriptions.

3.2 Data protection job description responsibilities

- Compliance with data protection legislation is the responsibility of all Employees/Staff of UNIPAKHELLAS
- The HR Department in collaboration with GDPR Owner/DPO and Compliance Officer of UNIPAKHELLAS shall organize a specific training and awareness session in relation to specific roles and Employees/Staff of UNIPAKHELLAS generally.
- Managers of each Company's function are responsible for ensuring that employees of their department have the appropriate training and awareness session in relation to their role. Together with HR Head Officer inform immediately Compliance Officer and GDPR Owner/DPO for the onboarding of new employees.
- Departments' Heads are also responsible for the retention of their department Register of Processing Activities (Section 12.2), which should be updated at least annually, or any time there is an amendment or addition and provided to Compliance Officer and GDPR Owner/DPO.
- Employees/Staff of UNIPAKHELLAS are responsible for ensuring that any personal data about them and supplied by them to UNIPAKHELLAS is accurate and up-to-date.

3.3 Data protection representative role and responsibilities

GDPR Owner/DPO

- The GDPR Owner/DPO, is designated responsible for managing compliance with UNIPAKHELLAS data protection policy on a day-to-day basis.

- The GDPR Owner/DPO has the following responsibilities:
  - Ensuring implementation of the data protection policy;
  - Development and review of the data protection policy;
  - Training and ongoing awareness as required by the data protection policy;
  - Approval of procedures where personal data is processed, such as:
  - The management and communication of privacy notices;
  - The handling of requests from individuals, including requests for access, rectification, erasure, etc.;
  - The collection and handling of personal data;
  - Complaints handling;
  - The management of security incidents; and
  - Outsourcing and off-shoring.
  - Liaison with those responsible for risk management and security issues within UNIPAKHELLAS;
  - Provision of expert advice and guidance on legislative and regulatory data protection matters;
  - The interpretation and application of the various exemptions applicable to the processing of personal data;
  - Advise and inform on the data protection impact assessment and monitor performance against the requirements of the EU GDPR;
  - Provision of advice in relation to data sharing projects (including security issues when data are off site);
  - Ensuring UNIPAKHELLAS has access to legislative updates and appropriate guidance related to data protection legislation;
  - Continually checking that UNIPAKHELLAS data protection regime reflects changes in legislation, practice and technology

- GDPR Owner/DPO responsibilities are assigned to a person who is suitably qualified and experienced, and appointed to take responsibility for UNIPAKHELLAS compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that UNIPAKHELLAS complies with the GDPR.

- GDPR Owner/DPO has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

- The GDPR Owner/DPO will maintain expert knowledge of data protection law and practices, as well as other professional qualities, to ensure that UNIPAKHELLAS complies with the requirements of the EU GDPR and relevant local data protection law(s) and regulations.

- Reporting directly to the Board of Directors the GDPR Owner/DPO must inform and advise on the protection of personal data in relation to the EU GDPR and Greek law(s) and regulations.

- The GDPR Owner/DPO will ensure that documentation to demonstrate compliance with the GDPR such as policies and procedures is kept up to date. For example, the register of processing activities required under Article 30. Furthermore, the GDPR Owner/DPO will plan and schedule data processing audits regularly, monitoring core activities to ensure they comply with the EU GDPR.

- The GDPR Owner/DPO is the main contact point for employees and will liaise with all members of staff on matters of data protection.

- Key tasks of the GDPR Owner/DPO (Article 39, (1) and Recital 97):

    - To inform and advise all members of staff on their obligation to adhere to the EU GDPR and local law(s) when dealing with personal data.
    - To monitor compliance with the EU GDPR and local law(s).
    - Advise and inform on data protection impact assessments (DPIA) where required, including monitoring performance of DPIAs against the requirements of the EU GDPR (Article 35.)
    - To be the point of contact for the data protection authority on issues relating to processing of personal data, and to consult with the data protection authority, where necessary, on any other personal data matters.
    - To contribute to the development and maintenance of all UNIPAKHELLAS data protection policies, procedures and processes in relation to the protection of personal data.
    - Advise management on the allocation of responsibilities internally to support ongoing compliance with the EU GDPR and local law(s).
    - Ensure training and awareness is available and delivered to all members of staff involved in processing operations relating to personal data.

- Regularly monitor compliance with the EU GDPR and local data protection law(s) by conducting audits of processes relating to personal data, and report to the Board of Directors.
- To be the point of contact for data subjects with regard to the processing of their personal data.
- To monitor compliance with the Data Protection Policy throughout UNIPAKHELLAS and to develop/advise on procedures for effective security.
- To advise senior management on the allocation of information security responsibilities.
- To develop/advise on formal procedures for reporting incidents (EU GDPR and information security-related) and investigations under Articles 33 and 34 of the GDPR.
- To contribute to the business continuity and disaster recovery planning process.
- To advise on and monitor the safeguarding of organizational record management, (Retention of Records of Processing Activities - Section 12.3)
- Work with information asset owners to ascertain the extent to which personal data is collected, held and/or used in UNIPAKHELLAS, and that it is properly controlled and safeguarded from loss of confidentiality, integrity or availability from any cause.
- To ensure that records of the processing are kept by UNIPAKHELLAS as detailed in GDPR Article 30 mentioned above.
- To advise the controller of its obligation to issue privacy notices to data subjects at the point of collection of their personal data under GDPR Articles 13 to 15.
- To review and appraise the soundness, adequacy and application of security and other controls for the protection of data.
- To identify and test the controls and, where appropriate, to suggest additional controls, which may be established to maintain the confidentiality, integrity and availability of personal data.
- To bring to the attention of the Compliance Officer and Board of Directors as appropriate any matters which are potential risk factors to the proper safeguarding of personal data within UNIPAKHELLAS

- The GDPR Owner/DPO is authorized to have access to all UNIPAKHELLAS's systems relating to the collection, processing and storage of personal data for the purpose of assessing the use and security of personal data. The GDPR Owner/DPO may expect the cooperation of all staff in carrying out these duties, including access to systems and records. In the event that cooperation is not being forthcoming, the GDPR Owner/DPO will report directly to Compliance Officer and the last will report to the Board of Directors accordingly.

4. POLICY MANAGEMENT PROCEDURE

The Data Protection Policy and GDPR arrangements are subject to development, review, evaluation and continuous improvement.

4.1 Responsibilities

- The GDPR Owner/DPO, is responsible for the Data Protection Policy, its development, review and evaluation.

- The IT Senior Manager is responsible for convening meetings of the Board of Directors either after there have been (or it is planned that there will be) significant changes in the organizational environment, business circumstances, legal conditions or technical environment, and which is likely to have an impact on the level of risk facing personal data. This role is also the defined owner of the Information Security Policy, is responsible for its development, review and evaluation.

4.2 Management Review

- Improving UNIPAKHELLAS's assessment of the risks, including updating the risk assessment and incident management plans.

- Any variations to the scope of the GDPR that may be required.

- Modifying or improving the policies and procedures and their effectiveness, ensuring that any changes to business or business processes, or changes to statutory, regulatory or contractual requirements are accommodated.

- Update of risk assessments, plans and related procedures.

- Modification of procedures and controls to respond to internal or external events that may impact compliance with the GDPR, including changes to:
    - Business and operational requirements
    - Risk reduction and security requirements
    - Operational conditions and processes
    - Legal and regulatory requirements
    - Contractual obligations
    - Levels of risk; criteria for accepting risks
    - Resource needs
    - Funding and budget requirements
- Reviewing and improving how the effectiveness of controls is measured.
- Improving the allocation of resources and responsibilities, including ensuring that complying with the GDPR is supported by adequate resources, funding and budget.
- Formulating and agreeing any changes to the Data Protection Policy which would be necessary to give effect to any improvements identified.

- The GDPR Owner/DPO is responsible for ensuring that:
    - Results of management reviews are communicated as appropriate to relevant interested parties;
    - Appropriate actions are taken as a result of management review.

The Board of Directors must approve any changes to the policy at its next scheduled meeting and prior to its implementation.

5. DATA PROTECTION PRINCIPLES

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Company's procedures are designed to ensure compliance with the principles.

5.1 Personal data collection principles

- Personal data must be processed lawfully, fairly and transparently
- Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.
- 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.
- The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.
- 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. UNIPAKHELLAS's Privacy Notice Procedure is set out in section 6.3.

5.2 Information that must be provided to the data subject

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 GDPR Owner/DPO;
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- The period for which the personal data will be stored most probably for five years' period;
- 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;

- The recipients or categories of recipients of the personal data, where applicable;
- Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- Any further information necessary to guarantee fair processing.

5.3 Lawful basis of personal data collection

- Personal data can only be collected for specific, explicit and legitimate purposes.
- Health related Personal Data

UNIPAKHELLAS may process health related Personal Data of Employees only for:

  - The proper implementation of law provisions, pensions, pension regulations or collective agreements which create rights dependent on the state of health of the Employee, or
  - The reintegration of or support for Employees or persons entitled to benefit in connection with sickness or work incapacity. Employee health related data will be treated as confidential.

- The information regarding an employee state of health shall only be processed by persons who are bound to secrecy by virtue of their office, profession or legal regulations or by virtue of an agreement, except insofar as they are obliged to disclose this information by law, or their task requires that this information should be disclosed to others who are authorized to process this information.

5.4 Accuracy of personal data

- 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 GDPR Owner/DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
- It is also the responsibility of the data subject to ensure that data held by UNIPAKHELLAS is accurate and up to date.

- All data subjects (Employees/customers/others) are required to notify UNIPAKHELLAS of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained. It is the responsibility of UNIPAKHELLAS to ensure that any notification regarding change of circumstances is recorded and acted upon.
- The GDPR Owner/DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, considering the volume of data collected, the speed with which it might change and any other relevant factors.
- On at least on annual basis, the GDPR Owner/DPO will review the retention dates of all the personal data processed by UNIPAKHELLAS, 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 section 12.
- The GDPR Owner/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 UNIPAKHELLAS decides not to comply with the request, the GDPR Owner/DPO must respond to the data subject to explain its reasoning and inform them of their right to complain to the data protection authority and seek judicial remedy.
- The GDPR Owner/DPO is responsible for making appropriate arrangements that, where third-party organizations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

5.5 Personal data minimization

- Personal data must be adequate, relevant and limited to what is necessary for processing.
- The GDPR Owner/DPO is responsible for ensuring that UNIPAKHELLAS 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 link to privacy statement and be approved by the GDPR Owner/DPO, unless a notification for the GDPR compliance has been already sent to the data subjects.

5.6 Personal data format

- Personal data will be retained in line with the Retention of Records Procedure (Section 12.2) and, once its retention date is passed, it must be securely destroyed as set out in this procedure.
- The GDPR Owner/DPO must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure (Section 12.2), and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation.

5.7 Secure processing of personal data

- Personal data must be processed in a manner that ensures the appropriate security.
- The GDPR Owner/DPO will carry out a risk assessment considering all the circumstances of UNIPAKHELLAS's controlling or processing operations.
- In determining appropriateness, the GDPR Owner/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 UNIPAKHELLAS itself, and any likely reputational damage including the possible loss of customer trust.
- When assessing appropriate technical measures, the GDPR Owner/DPO will consider the following:
    - The information protection requirements and good practice guidance, as presented in the Information Security Policy
    - Privacy; enhancing technologies such as pseudonymization and anonymization;
    - Identifying appropriate international security standards relevant to UNIPAKHELLAS.

- When assessing appropriate organizational measures the GDPR Owner/DPO will consider the following:
    - The appropriate training levels throughout UNIPAKHELLAS;
    - Measures that consider the reliability of employees (such as references etc.);
    - The inclusion of data protection 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 or make sure that access to portable electronic devices is secured through the use of personal unique access passwords;
- Restricting the use of employee's 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;
- The imposition of contractual obligations on the importing organizations to take appropriate security measures when transferring data outside the EEA.

- 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.

5.8 Demonstrating compliance

- The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)
- GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires the controller to demonstrate compliance with the principles and to state explicitly that this the controller's responsibility.
- UNIPAKHELLAS will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organizational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

6. PRIVACY

All processing of personal data by UNIPAKHELLAS is within the scope of this procedure.

6.1 Responsibilities

- The GDPR Owner/DPO is responsible for ensuring that the Privacy notices are correct and that mechanisms exist such as all data subjects are made aware of the contents of the notices prior UNIPAKHELLAS commencing collection of their data.
- All staff that need to collect personal data are required to follow this procedure.

6.2 Assessment Procedure for the legal basis of the processing of personal data

UNIPAKHELLAS identifies the legal basis for processing personal data before any processing operations take place by clearly establishing, defining and documenting:

- The specific purpose of processing the personal data and the legal basis to process the data under:
    - Consent (if applicable) obtained from the data subject;
    - Performance of a contract where the data subject is a party;
    - legal obligation that UNIPAKHELLAS is required to meet;
    - Protect the vital interests of the data subject, including the protection of rights and freedoms;
    - Official authority of UNIPAKHELLAS or to carry out the Processing that is in the public interest;
    - Necessary for the legitimate interests of the data controller or third party, unless the processing is overridden by the vital interests, including rights and freedoms;
    - National law.
    - Any special categories (if exist) of personal data processed and the legal basis to process the data under:
    - Explicit consent obtained from the data subject;
    - Necessary for employment rights or obligations;
    - Protect the vital interests of the data subject, including the protection of rights and freedoms;

- Necessary for the legitimate activities with appropriate safeguards;
- Personal data made public by the data subject;
- Legal claims
- Substantial public interest;
- Preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, provision of health or social care treatment, or management of health and social care systems and services, under the basis that appropriate contracts with health professionals and safeguards are in place;
- Public health, ensuring appropriate safeguards are in place for the protection of rights and freedoms of the data subject, or professional secrecy;
- National laws in terms of processing health data.

UNIPAKHELLAS records this information in line with its data protection impact assessment and data inventory (Section 16 and 15).

6.3 Privacy notices

When personal data collected from data subject with consent

- UNIPAKHELLAS is transparent in its processing of personal data and provides the data subject with the following:
  - identity, and contact details of the GDPR Owner/DPO and any data protection representatives;
  - The purpose(s), including legal basis, for the intended processing of personal data (section 6.4 below);
  - Where relevant, UNIPAKHELLAS's legitimate interests that provide the legal basis for the processing;
  - Potential recipients of personal data;
  - Any information regarding the intention to disclose personal data to third parties and whether it is transferred outside the EU;
  - Any other information required to demonstrate that the processing is fair and transparent.
- All information provided to the data subject is in an easily accessible format (either in a PDF document, printed letter, or email), using clear and plain language.
- UNIPAKHELLAS facilitates the data subject's rights in line with the data protection policy and the subject access request procedure (Section 7.1).
- Privacy notice for this personal data processing is recorded.

When data is contractually required for processing

- UNIPAKHELLAS processes data without consent in order to fulfil contractual obligations for instance but not limited to bank details to process salaries, distribution of any amounts, email address in order to contact customers of UNIPAKHELLAS, government issued identifiers, etc.
- Privacy notice for this personal data processing is recorded.

When personal data has been obtained from a source other than the data subject

- UNIPAKHELLAS makes clear the types of information collected as well as the source of the personal data (publicly accessible sources) and provides the data subject with:
    - The purpose(s), including legal basis, for the intended processing of personal data;
    - UNIPAKHELLAS's (data controller) identity, and contact details of the GDPR Owner/DPO and any data protection representatives;
    - Categories of personal data;
    - Any information regarding disclosing personal data to third parties and whether it is transferred outside the EU – UNIPAKHELLAS will provide information on the safeguards in place and how the data subject can also obtain a copy of these safeguards;
    - Any other information required to demonstrate that the processing is fair and transparent.

6.4 Conditions

- UNIPAKHELLAS provides the information stated in sections 6.2 and 6.3 above within:
    - One month of obtaining the personal data, in accordance with the specific circumstances of the processing;
    - At the first instance of communicating in circumstances where the personal data is used to communicate with the data subject;
    - When personal data is first disclosed in circumstances where the personal data is disclosed to another recipient.

- Sections 6.2 and 6.3 above do not apply:
  - If the data subject already has the information;
  - If the provision of the above information proves impossible or would involve an Excessive effort;
  - If obtaining or disclosure of personal data is expressly identified by Member State law; or
  - If personal data must remain confidential subject to an obligation of professional secrecy regulated by Member State law, including a statutory obligation of secrecy.

7. DATA SUBJECTS' RIGHTS

- Data subjects have the following rights regarding data processing, and the data that is recorded about them:
  - To make subject 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 take action to rectify and only after expiration of the period within which UNIPAKHELLAS is obliged to keep the personal data to block, erased, including the right to be forgotten, or destroy inaccurate data.
  - To request the data protection 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.

- UNIPAKHELLAS ensures that data subjects may exercise these rights:
  - Data subjects may make data access requests as described in Subject Access Request Procedure (Section 7.1); this procedure also describes how UNIPAKHELLAS will ensure that its response to the data access request complies with the requirements of the GDPR.

- Data subjects have the right to complain to UNIPAKHELLAS related to the processing of their personal data, the 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 (Section 7.2).

7.1 Subject Access Request Procedure

- All personal data processed by UNIPAKHELLAS is within the scope of this procedure.

- Data subjects are entitled to obtain:

  - Confirmation as to whether UNIPAKHELLAS is processing any personal data about that individual;
  - Access to their personal data;
  - Any related information;
  - The logic involved in any automated decisions relating to him or her.

Responsibilities

- The GDPR Owner/DPO is responsible for the application and effective working of this procedure, and for reporting to the Compliance Officer on Subject Access Requests (SARs).
- The GDPR Owner/DPO is responsible for handling all SARs.

Procedure

- Subject Access Requests are made using the e-mail account/address notified to all Data subjects, which is GDPR@unipakhellas.gr.

- The data subject specifies to UNIPAKHELLAS specific set of data held by UNIPAKHELLAS on their subject access request (SAR). The data subject can request all data held on them by filling the relevant Data Subject Request Form, which is provided by GDPR Owner/DPO upon data subject's request at GDPR@unipakhellas.gr.
- UNIPAKHELLAS records the date that the identification checks were conducted and the specification of the data sought.

- UNIPAKHELLAS provides the requested information to the data subject within one month from this recorded date. Under the GDPR Article 12 (3), that period may be extended by two further months where necessary, taking into account the complexity and number of the requests. UNIPAKHELLAS shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
- Once received, the subject access request (SAR) application is immediately forwarded to the GDPR Owner/DPO, who will ensure that the requested data is collected within the specified time frame recorded by UNIPAKHELLAS.

- Collection entails:

    - Collecting the data specified by the data subject, or
    - Searching all databases and all relevant filing systems (manual files) in UNIPAKHELLAS, including all back up and archived files (computerized or manual) and all email folders and archives. The GDPR Owner/DPO maintains a data map that identifies where all data in UNIPAKHELLAS is stored.
- The GDPR Owner/DPO maintains a record of requests for data and of its receipt, including dates in a “Data Subject Requests Record”.
- The GDPR Owner/DPO reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.
- If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:
    - National security
    - Crime and taxation
    - Health
    - Education
    - Social Work
    - Regulatory activity
    - Journalism, literature and art
    - Research history, and statistics
    - Publicly available information
    - Corporate finance
    - Examination marks
    - Examinations scripts
    - Domestic processing

- Confidential references
- Judicial appointments, honors and dignities
- Crown of ministerial appointments
- Management forecasts
- Negotiations
- Legal advice and proceedings
- Self-incrimination
- Adoption records
- Special educational needs
- Parental records and reports

- In the event that a data subject requests UNIPAKHELLAS to provide them with the personal data stored by the controller/processor, then UNIPAKHELLAS will provide the data subject with the requested information in electronic format, unless otherwise specified. The record should include the data subject's name and the date on which the information is delivered to the data subject.
- In the event that a data subject requests what personal data is being processed then UNIPAKHELLAS provides the data subject with the following information:
  - Purpose of the processing
  - Categories of personal data
  - Recipient(s) of the information, including recipients in third countries or international organizations
  - How long the personal data will be stored
  - The data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed, whenever and if applicable (i.e. after expiration of the period within which UNIPAKHELLAS is obliged to keep the personal data).
- UNIPAKHELLAS removes personal data from systems and processing operations as soon as a request for erasure has been submitted by the data subject.
- UNIPAKHELLAS contacts and communicates with other organizations, where the personal data of the data subject is being processed, to cease processing information at the request of the data subject.
- UNIPAKHELLAS takes appropriate measures without undue delay in the event that the data subject has: withdrawn consent if applicable (Section 8.2); objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.
- Information on the source of the personal data if it hasn't been collected from the data subject.

- Informs the data subject of any automated decision-making.
- If and where personal data has been transferred and information on any safeguards in place.

7.2 Complaints Procedure

This procedure addresses complaints from data subject(s) related to the processing of their personal data, UNIPAKHELLAS's handling of requests from data subjects, and appeals from data subjects on how complaints have been handled.

Responsibilities

- All Employees/Staff are responsible for ensuring any complaints made in relation to the scope of this procedure are reported to the GDPR Owner/DPO.
- The GDPR Owner/DPO is responsible for dealing with all complaints in line with this procedure.

Procedure

- UNIPAKHELLAS has the contact details of its GDPR Owner/DPO published on UNIPAKHELLAS website (https://unipakhellas.gr/) clearly in the Privacy Notice section.
- UNIPAKHELLAS clearly provides data subject(s) with the privacy notice (Privacy Notice) following its request by data subject(s)
- Data subjects are able to complain to UNIPAKHELLAS about:
    - How their personal data has been processed
    - How their request for access to data has been handled
    - How their complaint has been handled
    - Appeal against any decision made following a complaint.
- Data subject(s) lodging a complaint with the UNIPAKHELLAS's GDPR Owner/DPO are able to do so by via email direct to the GDPR Owner/DPO as published at UNIPAKHELLAS website (https://unipakhellas.gr/).
    - Complaints received via other paths are directed to the GDPR Owner/DPO for resolution.
    - Complaints are to be resolved within one (1) month.
    - Appeals on the handling of complaints are to be resolved within one (1) month.

- If UNIPAKHELLAS fails to act on a data subject's access request within the appropriate timeframe, or refuses the request, it sets out in clear and plain language the reasons it took no action/refusal. UNIPAKHELLAS will also inform the data subject(s) of their right to complain directly to the data protection authority. In doing so, UNIPAKHELLAS provides the data subject(s) with the contact details of the data protection authority and informs them of their right to seek judicial remedy.

7.3 Data Portability Procedure

- This procedure applies where a data subject exercises their right to data portability and applies to UNIPAKHELLAS (data controller) to receive their data in order to reuse or transfer it to other data controllers.

- Data subjects are entitled to ask:
  - For a copy of the personal data they have provided to UNIPAKHELLAS
  - For UNIPAKHELLAS to transmit the data to another data controller

- Within the scope of this procedure is any personal data concerning the data subject that:
  - He/she has provided to the data controller knowingly and actively, or through observations of his/her activities by virtue of the service of UNIPAKHELLAS;
  - Has been processed through automated means; and
  - Has been processed on the basis of the data subject's consent or a contract to which the data subject is a party.

- This procedure will most commonly be used when transmitting data directly to another data controller.
- This procedure also applies to circumstances when UNIPAKHELLAS is the "receiving data controller". That is, when personal data from another data controller is received due to the data subject exercising their right to data portability.

Responsibilities

- UNIPAKHELLAS is responsible for transmitting the data without hindrance and ensures that it is transmitted with the appropriate level of security (e.g. through an authenticated communication with the necessary level of data encryption). UNIPAKHELLAS should assess the specific risks linked with data portability and take appropriate risk mitigation measures.

- The GDPR Owner/DPO of UNIPAKHELLAS is responsible for the application and effective working of this procedure, and for reporting performance to the Compliance Officer.

Procedure

- UNIPAKHELLAS informs data subjects of the existence of the new right to portability at the time where personal data is obtained.
- Any request is immediately forwarded to the GDPR Owner/DPO to ensure that the requested data is provided/transmitted within the timeframe noted.
- UNIPAKHELLAS chooses whether to request that the data subject provide evidence of their identity in the form to be decided by the GDPR Owner/DPO.
- Where the data requested concerns a third party (ies), the GDPR Owner/DPO reviews whether or not transmitting data to another data controller would cause harm to the rights and freedoms of other data subjects.
- The data subject identifies the personal data that is to be transmitted or provided for their own use.
- The GDPR Owner/DPO maintains a record of requests for data and of its receipt, including dates.
- UNIPAKHELLAS has set safeguards that ensure the personal data transmitted are only those that the data subject has requested to be transmitted.
- The requested information is provided to the data subject in structured, commonly used and machine readable format that allows for the effective re-use of the data. UNIPAKHELLAS retains a register of such file formats electronically.
- When transmitting data to another data controller, UNIPAKHELLAS forwards the data in an interoperable format. In the event that technical impediments prohibit direct transmission, UNIPAKHELLAS explains these impediments to the data subject(s).

- UNIPAKHELLAS provides the requested information within one month from the request date. If the request is complex, UNIPAKHELLAS can extend this time frame to (maximum) three months. UNIPAKHELLAS informs the data subject of the reasons for the delay via e-mail within one month of the original request.
- The request does not affect the original retention period that applies to the data that has been transmitted.

Receiving personal data

- UNIPAKHELLAS does not by default accept and process personal data received from another data controller following a personal data request nor does it retain all the data received.
- UNIPAKHELLAS only accepts and retains data that is necessary and relevant to the service being provided.
- If data received contains third-party data, UNIPAKHELLAS keeps the data under the sole control of the requested user. This data is only managed for their needs and not for purposes other than those of UNIPAKHELLAS.
- UNIPAKHELLAS provides data subject(s) with information about the personal data relevant for the performance of their services, limiting risks posed to third parties and unnecessary duplication of personal data.

7.4 Subject Right to be forgotten

- All personal data processed by UNIPAKHELLAS is within the scope of this procedure after expiration of the period within which UNIPAKHELLAS is obliged to keep such personal data.
- UNIPAKHELLAS must comply with an individual's request for deletion or removal of personal data where there is no compelling reason for its continued processing.
- When:
    - The personal data is no longer necessary for the purpose for which it was originally processed
    - Consent, if applicable, is withdrawn
    - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
    - The personal data was unlawfully processed
    - The personal data has to be erased in order to comply with a legal obligation.

- There are some specific circumstances where the right to erasure does not apply and UNIPAKHELLAS can refuse to deal with a request. UNIPAKHELLAS can refuse to comply with a request for erasure where the personal data is processed for the following reasons:
- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- The exercise or defense of legal claims.

Responsibilities

- The GDPR Owner/DPO is responsible for the application and effective working of this procedure, and for reporting to the Compliance Officer on Right to be forgotten requests.
- The GDPR Owner/DPO is responsible for handling all Right to be forgotten requests.

Procedure

- The data subject provides UNIPAKHELLAS with evidence of their identity, in the form to be decided by UNIPAKHELLAS.
- UNIPAKHELLAS initiates the deletion of all related data and provides the verification of deletion to the data subject within one month from this request date. Under the GDPR Article 12 (3), that period may be extended by two further months where necessary, taking into account the complexity and number of the requests. UNIPAKHELLAS shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
- Once received, the Right to be forgotten request application is immediately forwarded to the GDPR Owner/DPO, who will ensure that the personal data of the data subject was deleted within the specified time frame by UNIPAKHELLAS.

- Deletion entails:
  - The destruction of all personal data of the data subject,
  - The destruction of all related data of the data subject by searching all databases and all relevant filing systems (manual files) in UNIPAKHELLAS, including all back up and archived files (electronic or manual) and all email folders and archives. The GDPR Owner/DPO maintains a data map that identifies where all data in UNIPAKHELLAS is stored.
  - Requesting the deletion and the verification of the deletion of all related data of the data subject from third parties that UNIPAKHELLAS is associated with.

7.5 Restriction of Processing Procedure

This procedure addresses requests from data subject(s) related to the restriction of processing of their personal data and UNIPAKHELLAS's handling of such requests from data subjects.

Responsibilities

- All Employees/Staff are responsible for ensuring any requests made in relation to the scope of this procedure are reported to the GDPR Owner/DPO.
- The GDPR Owner/DPO is responsible for dealing with all requests for restriction of processing in line with this procedure.

Procedure

- UNIPAKHELLAS has the contact details of its GDPR Owner/DPO published on UNIPAKHELLAS website (https://unipakhellas.gr/) clearly in the Privacy Notice.
- Data subjects have the right to request the restriction or suppression of their personal data processed by UNIPAKHELLAS about.
- This right is not an absolute right of the data subject and only applies under certain circumstances. These circumstances are outlined below:

  - The data subject contests the accuracy of the personal data, and wants processing to be restricted for a period of time, until the accuracy of the personal data is verified by UNIPAKHELLAS;
  - The processing is unlawful but the data subject objects to the erasure of their data and requests the restriction of their use instead;

- The personal data is no longer needed for the purposes of processing, but the data subject requires their personal data for the establishment, exercise or defense of legal claims;
- The data subject has objected to processing which is based on UNIPAKHELLAS legitimate interests, pending the verification of that objection.

- Although this is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:
  - If an individual has challenged the accuracy of their data and asked for their rectification (Article 16), they also have a right to request UNIPAKHELLAS restricts processing while they consider their rectification request; or
  - If an individual exercises their right to object under Article 21(1), they also have a right to request you restrict processing while you consider their objection request.

- Data subject(s) lodging a request to restrict processing with the UNIPAKHELLAS's GDPR Owner/DPO are able to do so via email direct to the email address: gdpr@unipakhellas.gr
  - Requests to restrict processing received are directed to the GDPR Owner/DPO for resolution.
  - Requests to restrict processing are to be responded to within one (1) calendar month.
  - Appeals on the handling of requests to restrict processing requests are to be resolved within one (1) calendar month

- The restriction of data can happen in any of the following ways:
  - Temporarily moving the data to another processing system; or
  - Making the data unavailable to users through technical configuration;

- Once restriction is in place UNIPAKHELLAS should also note on their systems that the processing of the data has been restricted.
- If UNIPAKHELLAS fails to act on a data subject's restriction of processing request within the appropriate timeframe, or refuses the request, it sets out in clear and plain language the reasons it took no action/refusal. UNIPAKHELLAS will also inform the data subject(s) of their right to complain directly to the data protection authority. In doing so, UNIPAKHELLAS provides the data subject(s)

with the contact details of the data protection authority and informs them of their right to seek judicial remedy.

8. CONSENT

- UNIPAKHELLAS 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.
- UNIPAKHELLAS understands ‘consent’ to mean that the data subject has been fully informed of the intended 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.
- 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 (Consent Procedure – Section 8.1) of data subjects must be obtained unless an alternative legitimate basis for processing exists.

8.1 Consent Procedure

- The consent of the data subject is one of the conditions for the processing of his or her personal data and is within the scope of this procedure. UNIPAKHELLAS needs to obtain consent when no other lawful basis applies.
- Consent of the data subject is defined by the GDPR as “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”.
- Explicit consent is required for the processing of sensitive personal data. Specific conditions apply to the validity of consent given by children in relation to information society services, with requirements to obtain and verify parental consent below certain age limits.

Responsibilities

- As a data controller, UNIPAKHELLAS is responsible under the GDPR for obtaining consent from the data subject under advisement from GDPR Owner/DPO.

Consent procedure

- UNIPAKHELLAS provides a clear privacy notice wherever personal data is collected (Privacy Notice Document) to ensure that consent is informed and that the data subject is informed of their rights in relation to their personal data.
- UNIPAKHELLAS demonstrates data subject(s) consent to the processing of his or her personal data or explicit consent for sensitive personal data.
- UNIPAKHELLAS demonstrates data subject(s) consent to the processing of his or her personal data for one or more specific purposes.
- UNIPAKHELLAS demonstrates data subject(s) consent is clearly distinguishable from any other matter relating to the data subject (if recorded in paper / electronic file format use a Data Subject Consent Form, or email then attach the email to the form).
- UNIPAKHELLAS demonstrates data subject(s) consent is intelligible and accessible using clear and plain language.
- UNIPAKHELLAS demonstrates data subject(s) are informed of their right to withdraw consent before giving consent (Right to withdraw Consent Procedure – Section 8.2).
- UNIPAKHELLAS demonstrates processing of data is limited to that stated in the contract, bound by the explicit consent given by the data subject.

8.2 Withdrawal of Consent Procedure

- This procedure addresses the data subject(s) right to withdraw consent for the processing of his or her personal data.
- Withdrawal of consent by the data subject means an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies withdrawal of consent to the processing of personal data relating to him or her.
- Withdrawal of consent shall be without effect to the lawfulness of processing based on consent before its withdrawal. Whereas consent covered all processing activities carried out for the same purpose or purposes, withdrawal of consent covers all processing activities carried out for the same purpose or purposes.

Responsibilities

- As a data controller, UNIPAKHELLAS, is responsible under the GDPR for administering withdrawal of consent from the data subject under advisement from GDPR Owner/DPO.

Withdrawal of consent procedure

- UNIPAKHELLAS demonstrates the data subject has withdrawn consent to the processing of his or her personal data.
- Where the processing had multiple purposes, UNIPAKHELLAS demonstrates withdrawal of consent for each purpose.
- The processing activities that relied upon the consent is stopped in accordance with the relevant process. The GDPR Owner/DPO will inform the relevant process owner of this change so that processing can be stopped.

9. SECURITY OF DATA

- All Employees/Staff are responsible for ensuring that any personal data which UNIPAKHELLAS 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 authorized by UNIPAKHELLAS to receive that information and has entered into a confidentiality agreement, or a service agreement which should include a confidentiality undertaking or undertaking in accordance with the applicable GDPR legislation.
- All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Policies of the Group. All personal data should be treated with the highest security and must be kept:
    - In a lockable room with controlled access; and/or
    - In a locked drawer or filing cabinet; and/or
    - If electronic, password protected in line with corporate requirements; and/or
    - Stored on (removable) computer media which are encrypted in line with best practice.

- Care must be taken to ensure that PC screens and terminals are not visible except to authorized Employees/Staff of UNIPAKHELLAS. All Employees/Staff and Customers are provided by the Head IT a personal unique password for getting access to organizational information of any sort and instructions for rules, on screen time-outs etc (screen lock policy).
- Manual records may not be left where they can be accessed by unauthorized personnel and may not be removed from business premises without explicit authorization. As soon as manual records are no longer required for day-to-day customer support, they must be removed from secure archiving.
- Personal data may only be deleted or disposed of in line with the Retention of Records Procedure (Section 12.2). 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 before disposal.
- Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorized to process data off-site.

10. DISCLOSURE OF DATA

- UNIPAKHELLAS must ensure that personal data is not disclosed to unauthorized 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 and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of UNIPAKHELLAS's business.
- All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorized by the GDPR Owner/DPO.

11. PERSONAL DATA BREACH NOTIFICATION PROCEDURE

- This procedure applies in the event of a personal data breach under Article 33 of the GDPR – Notification of a personal data breach to the data protection authority – and Article 34 – Communication of a personal data breach to the data subject.
- The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognize that not all organizations involved in the processing of personal data have the same degree of responsibility. Each organization should

establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

11.1 Responsibility

- All users (whether Employees/Staff, contractors or temporary Employees/Staff and third party users) and owners of UNIPAKHELLAS are required to be aware of, and to follow this procedure in the event of a personal data breach (reference Training Policy – Section 14).

- All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the GDPR Owner/DPO who will communicate immediately the breach to the Compliance Officer, General Manager and Head of IT.

11.2 Procedure – Breach notification data controller to data protection authority

- UNIPAKHELLAS determines if the data protection authority need to be notified in the event of a breach.
- UNIPAKHELLAS assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting data protection impact assessment against the breach and/or other means available.
- If a risk to data subject(s) is likely, UNIPAKHELLAS reports the personal data breach to the data protection authority without undue delay, and not later than 72 hours.
- If the data breach notification to the data protection authority is not made within 72 hours, UNIPAKHELLAS's GDPR Owner/DPO submits it electronically via email with a justification for the delay.
- If it is not possible to provide all of the necessary information at the same time UNIPAKHELLAS will provide the information in phases without undue further delay.
- The following information needs to be provided to the data protection authority:
    - A description of the nature of the breach.
    - The categories of personal data affected.
    - Approximate number of data subjects affected.
    - Approximate number of personal data records affected.
    - Name and contact details of the GDPR Owner/DPO.

- Consequences of the breach.
- Any measures taken to address the breach.
- Any information relating to the data breach.

- The GDPR Owner/DPO notifies the Data Protection Authority.
- The breach notification is made by email or by submitting it in Data Protection Authority Headquarters'
- A confirmation of receipt of this information should be received by the GDPR Owner/DPO in the form provided by Law or any circulars/directives issued by the Data Protection Authority.

11.3 Procedure – Breach notification data controller to data subject

- If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, UNIPAKHELLAS notifies those/the data subjects affected immediately.
- The notification to the data subject describes the breach in clear and plain language, in addition to information specified in section 11.2:
  - UNIPAKHELLAS will revoke all access of the specific personal data for all users and simultaneous stopping of all services running by the corresponding data sectors, leaving with access only the administrator temporarily.
  - UNIPAKHELLAS takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely.

- If the breach affects a high volume of data subjects and personal data records, UNIPAKHELLAS makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder the UNIPAKHELLAS's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.
- If UNIPAKHELLAS has not notified the data subject(s), and the data protection authority considers the likelihood of a data breach will result in high risk, UNIPAKHELLAS will communicate the data breach to the data subject without undue delay.
- UNIPAKHELLAS documents any personal data breach (es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

12. RETENTION AND DISPOSAL OF DATA

- UNIPAKHELLAS shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.
- UNIPAKHELLAS 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 organizational measures to safeguard the rights and freedoms of the data subject.
- UNIPAKHELLAS's data retention and data disposal procedures will apply in all cases.
- Personal data must be disposed of securely in accordance with the sixth principle of the GDPR processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.
- All UNIPAKHELLAS's records, whether analogue or digital, are subject to the retention requirements of this procedure.

12.1 Responsibilities

- The following roles are responsible for retention of these records as they are the information asset owners.
    - Asset owners are/responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR.
    - Departments' Heads are also responsible for the retention of their department Register of Processing Activities, which should be updated any time there is an amendment or addition and provided to Compliance Officer and GDPR Owner/DPO. The GDPR Owner/DPO is responsible for retention of all other statutory records.
    - The GDPR Owner/DPO and Compliance Officer are responsible for storage of data in line with this procedure.

12.2 Procedure

- The required retention periods, by record type, are recorded in Record of Processing Activities (RoPA) under the following categories:
    - Record type
    - Retention period
    - Retention period to start from (at creation, submission, payment, etc.)
    - Retention justification

- Record medium
- Disposal method

- Each data asset that is stored is marked with the name of the record, the record type, the original owner of the data, the information classification, the location of storage, the required retention period, the planned date of destruction, and any additional special information.

- The GDPR Owner/DPO and persons under 12.1 of this Policy are responsible for destroying data once it has reached the end of the retention period. Destruction must be completed within 30 days of the planned retention period.

- Portable/removable storage media are destroyed in line with Secure Disposal of Storage Media best practice.

13. 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 transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:
    1. Assessment of adequacy by the data controller assessing adequacy, the EU based exporting controller should take account of the following factors:
        a. the nature of the information being transferred;
        b. the country or territory of the origin, and final destination, of the information;
        c. how the information will be used and for how long;
        d. the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
        e. the security measures that are to be taken as regards the data in the overseas location such as:
        f. Binding corporate rules - UNIPAKHELLAS may adopt approved binding corporate rules for the transfer of data outside the EU.
        g. Model contract clauses - UNIPAKHELLAS may adopt approved model contract clauses for the transfer of data outside of the EEA.
        h. Exception

2. In the absence of binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organization shall only take place on one of the following conditions:
    a. The data subject is not opposed 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;
    b. The transfer is took place
    c. The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
    d. 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;
    e. The transfer is necessary for important reasons of public interest;
    f. The transfer is necessary for the establishment, exercise or defence of legal claims; and/or
    g. 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.

14. TRAINING POLICY/PROCEDURE

This policy applies to UNIPAKHELLAS's training and awareness program where relevant to the GDPR, compliance with the GDPR, and other matters relating to data protection and privacy

- The GDPR Owner/DPO assigns data protection responsibilities to Employees/Staff in relation to UNIPAKHELLAS's policies and procedures on personal data management.
- The GDPR Owner/DPO shall ensure that all Employees/Staff with day-to-day responsibilities involving personal data and processing operations, and those with permanent/regular access to personal data, demonstrate compliance with the GDPR.
- These members of Staff are able to demonstrate competence in their understanding of the GDPR and how this is practiced and implemented throughout UNIPAKHELLAS.
- The GDPR Owner/DPO ensures that these members of Employees/Staff are kept up to date and informed of any issues related to personal data.

- The GDPR Owner/DPO maintains a list of relevant external bodies, the most important of which is the Data Protection Authority in Greece.
- The GDPR Owner/DPO in collaboration with HR Department promote training and awareness programs, and UNIPAKHELLAS shall make resources available in order to raise awareness. The GDPR Owner/DPO shall demonstrate and communicate to Employees/Staff the importance of data protection in their role and ensure that they understand how and why personal data is processed in accordance with UNIPAKHELLAS's policies and procedures.
- The GDPR Owner/DPO ensures that all security requirements related to data protection are demonstrated and communicated to Employees/Staff to the same affect.
- Employees/Staff are provided with specific training on processing personal data relevant to their individual day-to-day roles and responsibilities, and in accordance with UNIPAKHELLAS' policies and procedures.
- Employees/Staff are provided with specific training on any information security requirements and procedures applicable to data protection and the data processing within their individual day-to-day roles and responsibilities, including reporting personal data breaches.
- Employees/Staff are provided with training on dealing with complaints relating to data protection and processing personal data.
- The GDPR Owner/DPO retains records of the relevant training undertaken by each person who has this level of responsibility.
- All Employees/Staff with day-to-day responsibilities involving personal data and processing operations will at planned intervals assess the capability of any systems used to record personnel information, to demonstrate compliance to the GDPR.
- The GDPR Owner/DPO is responsible for organizing relevant training any time there is an amendment to GDPR legal framework for all responsible individuals and Employees/Staff generally, and for maintaining records of the attendance of staff at relevant training at appropriate times.

15. INFORMATION ASSET REGISTER/DATA INVENTORY

- UNIPAKHELLAS has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. UNIPAKHELLAS's data inventory and data flow determines :
    - Business processes that use personal data;
    - Source of personal data;
    - Volume of data subjects;

- Description of each item of personal data;
- Processing activity;
- Maintains the inventory of data categories of personal data processed;
- Documents the purpose(s) for which each category of personal data is used;
- Any data transfers; and
- All retention and disposal requirements.

- UNIPAKHELLAS is aware of any risks associated with the processing of particular types of personal data.
- UNIPAKHELLAS assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs– Section 16) are carried out in relation to the processing of personal data by UNIPAKHELLAS and in relation to processing undertaken by other organisations on behalf of UNIPAKHELLAS.
- UNIPAKHELLAS shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.
- Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, UNIPAKHELLAS shall, prior to the processing, ad hoc carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.
- Where, as a result of a DPIA it is clear that UNIPAKHELLAS is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not UNIPAKHELLAS may proceed must be escalated for review to the GDPR Owner/DPO.
- Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to UNIPAKHELLAS's documented risk acceptance criteria and the requirements of the GDPR.

16. DATA PROTECTION IMPACT ASSESSMENT

In projects that involve processing personal data, or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects are within the scope of this procedure and will be subject to a data protection impact assessment (DPIA). The GDPR Owner/DPO in collaboration with Compliance Officer shall provide consultation and/or recommend actions and steps to be followed and is in charge for monitoring and supervising implementation of all below.

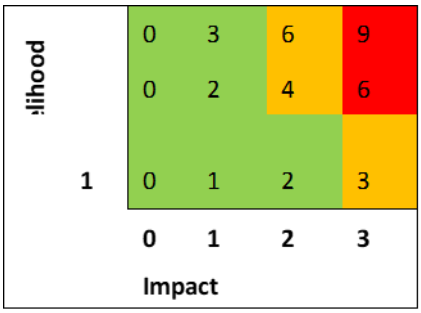
16.1 Responsibilities

I. The GDPR Owner/DPO is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.
II. The GDPR Owner/DPO is responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.
III. The GDPR Owner/DPO together with the Compliance Officer and the Head of Legal are responsible for implementing any privacy risk solutions identified.

16.2 Procedure

- The GDPR Owner/DPO identifies the need for a DPIA at the start of each project, by assessing the project and type of personal data involved, or processing activity.
- Using the criteria below, following the likelihood and impact matrix, UNIPAKHELLAS defines the risks to rights and freedoms of data subjects as:

Likelihood and impact matrix:



Risks to rights and freedoms of data subjects:

Risk Level	From	To	GDPR Assessment
High	6	9	Highest unacceptable risk
Medium	3	5	Unacceptable risk
Low	1	2	Acceptable risk
Zero	0	0	No risk

16.3 Identify privacy risks

- UNIPAKHELLAS assesses the privacy risks for each process activity as described in section 16.2 above by:
  - Identifying and describing the privacy risk associated to that process activity
  - Using the likelihood criteria (1 – low, 2 – medium and 3 - high), scoring the likelihood of the risk occurring
  - Using the impact criteria (0 – zero impact, 1 – low, 2 – medium and 3 - high) of the risk should it occur
  - Producing a calculated risk, identifying the risk to the rights and freedoms of data subjects.
- In assessing the privacy risks, UNIPAKHELLAS considers: risks to the rights and freedoms of natural persons resulting from the processing of personal data; risks to the business (including reputational damage); and its objectives and obligations (both regulatory and contractual).
- UNIPAKHELLAS identifies solutions to privacy risks, assigns a risk treatment owner and sets a target date for completion.
- UNIPAKHELLAS prioritizes analyzed risks for risk treatment based on the risk level criteria established in section 16.2 above.
- UNIPAKHELLAS approves and signs off each DPIA for each data processing activity. The Compliance Officer may sign off reviews that took place, but assessments should be signed off by UNIPAKHELLAS.

17. REGULATORY INTERVENTIONS PROCEDURE

- Response to regulatory interventions by the data protection authority should be managed by the GDPR Owner/DPO of the Company on the basis of a clear and established procedure. This procedure should include the:
  - Analysis of the regulatory recommendations and requirements.
  - Extraction of all action points and their assessment to establish which can be tackled together.
  - Establishment of the current state and target state of the organization.
  - Identification of gaps.
  - Development of individual remediation projects and action plans.
  - Engagement of specialist resources and project/program management to ensure the successful delivery of the regulatory solution.
  - Cooperation and coordination of the effort to address all remediation points.
  - Tracking and validation of all remedial actions taken.

18. DOCUMENT OWNER

UNIPAKHELLAS is the owner of this document and the GDPR Owner/DPO is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff of UNIPAKHELLAS.