DATA PROTECTION POLICY

INSURANCE ASSOCIATION OF CYPRUS

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, that they receive adequate information in relation to the processing of their data and that they can exercise rights in relation to their personal data.

1.2. Definitions used by the organisation (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.

1.3. 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.
- 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 organisation.
- Processing – any operation or set of operations which is performed on personal data or on sets of personal data, by automated means or otherwise, 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.
- 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.

- Information asset/system Owner – is the person responsible for ensuring that the asset / system is managed appropriately, to meet the requirements of the organisation, is properly protected and that risks and opportunities are monitored.
- 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.
- Information System – is a system related with the processing of information with the use of application software, system software, information technology, services, and hardware for purpose of addressing specific goals of the Group of Companies. All information systems must have a nominated owner.
- Information asset - a body of information, defined and managed as a single unit. All information assets must have a nominated owner.
- Asset Owner – The person(s) responsible for a processing operation as designated by the Personal Data Operations Register
- Management – Director General of the Association

2. Policy statement

2.1. Policy statement

- The Board of Directors and the Director General of the Insurance Association of Cyprus ("Association" or "you"), located at 23, Zenon Sozos Street 1st Floor, 1516 Nicosia, Cyprus, is committed to compliance with the EU and Cypriot legal and regulatory framework (including but not limited to the GDPR and Act 125(I)/2018) governing the processing of personal data, and the protection of the "rights and freedoms" of individuals whose information the Insurance Association of Cyprus collects and processes.
- Compliance with the legal and regulatory framework governing the processing of personal data, including but not limited to the GDPR is described by this Policy and other relevant policies, along with any connected processes and procedures.
- This Policy applies to all of the Insurance Association of Cyprus' personal data processing functions, including those performed on members', employees', suppliers' and partners' personal data, and any other personal data the organisation processes which come from competent authorities and/or other stakeholders that the Association liaises with in order to carry out its mission and functions.
- Partners and any third parties working with or for Insurance Association of Cyprus, and who have or may have access to personal data, will be expected to enter into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which the Insurance Association of Cyprus is committed, and which gives the Association the right to monitor compliance with the terms of the agreement.

3. Responsibilities and roles under the General Data Protection Regulation

3.1. Association's and Employees' responsibilities

- **The Insurance Association of Cyprus** is a data controller under the GDPR. Asset Owners act as data processors for the Association for their respective processing operations as stipulated in the Personal Data Operations Register and in that capacity they are responsible for ensuring compliance with the provisions

of the present Policy and any subsequent amendments thereof as shall be approved by the Board of Directors.

The Management of the **Insurance Association of Cyprus** is responsible for developing and encouraging good information handling practices within the **Insurance Association of Cyprus**; responsibilities are set out in herein.

- Compliance with data protection legislation is the responsibility of all employees of the Insurance Association of Cyprus who process personal data.
- The Management of the Association, with the assistance of the asset owner responsible for human resources issues sets out specific training and awareness requirements in relation to the obligations of the Association's employees in relation to the handling and processing of personal data.
- All employees of the Insurance Association of Cyprus are responsible for providing accurate personal data concerning them or others to the Insurance Association of Cyprus and verify their validity upon requestof the asset owner responsible for human resources issues or inform the organization for any necessary changes.

4. Policy Management Procedure

4.1. Scope

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

4.2. Responsibilities

- The Management is responsible for the development, review and evaluation of this Policy. The Management may seek the assistance and/or the recommendations of the legal and regulatory affairs asset owner(s) of the Association
- The Management is responsible for the implementation of this Policy in order to ensure compliance with the GDPR.
- Asset Owners in their respective areas of expertise are responsible for informing the Management in case significant changes in the organisational environment, business circumstances, legal conditions or technical environment are effected or are contemplated which are likely to have an impact on the level of personal data risk.

4.3. Management reviews

- Management reviews consider:
    - Changes in internal and external issues relevant and/or affecting data protection issues(e.g. changes in the legal and/or regulatory requirements, operational changes in the organisation and/or expansion of activities etc);
    - Information on GDPR performance.
- Performance for GDPR compliance is evaluated considering:
    - Need for change and/or amendments on Data Protection policy and objectives;
    - Techniques or services which could improve compliance with the GDPR;
    - Risks or issues arising from assumption of new responsibilities or the provision of new services;
    - Changes (internal or external) that could affect compliance with GDPR;
    - Adequacy of the Data Protection Policy;

- Recommendations for improvement (internally or externally generated);
- Actions arising from disruptive incidents (post-incident reports);
- Emerging good practice and guidance.

4.4. Management review outputs

- Should it prove necessary the Management may promote changes in relation but not limited to the following matters:
- Modifying or improving the Policies and procedures to ensure that any changes to business or business processes, or changes to statutory, regulatory or contractual requirements are accommodated.
- Procedures and controls, in order to respond to internal or external events that may impact compliance with the GDPR, including changes to:
  - Business and operational requirements
  - Risk exposure and security requirements
  - Operational conditions and processes
  - Legal and regulatory requirements
  - Contractual obligations
  - Resource needs
  - Funding and budget requirements.
- Formulating and agreeing any changes to the Data Protection Policy which would be necessary to give effect to any improvements identified.

The Board of Directors will approve the Data Protection Policy of the Association and any subsequent amendments to it. The Management will also notify the Board of Directors of any issues related to and/or involving the processing of personal data by the Association.

5. Data protection principles

- All processing of personal data is conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Insurance Association of Cyprus' policies and procedures are designed to ensure compliance with the principles.

5.1. Personal data collection principles

- Personal data must be processed lawfully, fairly and transparently.
- Lawfully – 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. 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. Insurance Association of Cyprus' Privacy Notice Procedure is set out in section **Error! Reference source not found.**.

5.2. Lawful basis of personal data collection

- 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 the initial purpose.

5.3. 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 Management, with the assistance of the asset owner responsible for human resources issues 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 Insurance Association of Cyprus is accurate and up to date.
- Directors, Committee Members, employees, associates and vendors who provide services to the Association are required to notify the Insurance Association of Cyprus of any changes in their circumstances to enable personal records to be updated accordingly. It is the responsibility of the Association to ensure that any notification regarding change of circumstances is recorded and acted upon.
- The Management with the assistance of asset owners of processing operations are 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.
- Personal Data of Directors, Committee Members, employees or vendors/partners/associates that is no longer required will be securely deleted/destroyed in line with section 14 subject to Management notification and approval
- The Management is responsible for responding to requests for exercise of rights in relation to personal data from data subjects, within one month, as per section 8.3. In performing this task the Management may request the assistance of the legal and regulatory affairs asset owner who may prepare a draft reply for Management review and approval. Any written replies to data subjects shall be signed by the Management representing the Association, the Data Controller. If there are actions that need to be taken, the Management shall then request the asset owners involved to perform any action necessary to comply with the data subject's request in line with the reply of the Association to the data subject.

5.4. Personal data minimization

- Personal data must be adequate, relevant and limited to what is necessary for processing. The Insurance Association of Cyprus does not collect information that is not strictly necessary for the purpose for which it is obtained.

5.5. Personal data format

- Personal data will be retained in line with the Retention of Data Procedure (Section 14) and, once its retention date is passed, it must be securely destroyed as set out in this procedure.
- The Management with assistance and/or acting on the advice of the legal and regulatory affairs asset owner(s) must specifically approve any data retention that exceeds the retention periods defined in Retention of Data Procedure (Section 14.2) , 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.

5.6. Secure processing of personal data

- Personal data must be processed in a manner that ensures the appropriate security.
- The Insurance Association of Cyprus outsources IT security of processing issues and as a minimum the vendor offering IT and IT security services to the Association should apply appropriate and GDPR compliant security measures and standards relevant to the Association and consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or members) if a security breach occurs, the effect of any security breach on the Insurance Association of Cyprus itself, and any likely reputational damage, obligations that are reflected in the IT security agreement of the Association and the vendor in question.
- When assessing appropriate organisational measures the Management with the assistance of the asset owner for human resources issues, the Health and Safety asset owner (where applicable), the IT Security Officer and the lawyers/legal advisors of the Association will consider the following:
  - The appropriate training levels throughout the Insurance Association of Cyprus;
  - Measures that consider the reliability of employees (such as references etc.);
  - The inclusion of data protection clauses in employment contracts;
  - Identification of 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 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;
- 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.

5.7. Demonstrating compliance

- The controller must be able to demonstrate compliance with the GDPR's other principles (accountability), as per Article 5(2).
- The Insurance Association of Cyprus will demonstrate compliance with the data protection principles by implementing the data protection policy, implementing technical and organisational measures such as data protection by design, DPIAs where required in accordance to the risk based approach adopted by the Association, breach notification procedures and incident response plans.

6. Procedure for the Assessment of Legal Basis

6.1. Scope

- The assessment and identification of the legal basis for the activities processing personal data of the Association is within the scope of this procedure.

6.2. Responsibilities

- The Association is responsible for ensuring that the legal basis for processing of personal data is identified correctly, prior to commencing the processing of personal data.

6.3. Assessment Procedure for the legal basis of the processing of personal data

- The Insurance Association of Cyprus identifies the legal basis for processing personal data before any processing operation takes place by clearly establishing, defining and documenting:

- The specific purposes of processing the personal data and the legal basis to process the data under:
  - Consent obtained from the data subject;
  - Performance of a contract where the data subject is a party;
  - Legal obligation that the Association is required to meet;
  - Duty to protect the vital interests of the data subject, including the protection of rights and freedoms;
  - Official authority of the Association to carry out processing that is in the public interest;
  - 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 of personal data processed and the legal basis to process the data under:
  - Explicit consent obtained from the data subject;
  - Necessary for compliance with legal and regulatory obligations of the Association in the field of employment law;
  - 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.

- Insurance Association of Cyprus records this information in the information asset/personal data operations register (Sections 18 and 13).

7. Information provided to Data Subjects – Privacy Notice

7.1. Scope

- Insurance Association of Cyprus is responsible to provide the data subjects with information regarding the processing of their personal data.

7.2. Responsibilities

- The Insurance Association of Cyprus is responsible for ensuring that the privacy notice is made readily available to all data subjects.
- All staff that need to collect personal data are required to follow this procedure.

7.3. Privacy Notice Information provision

- The Insurance Association of Cyprus is transparent in its processing of personal data and provides the data subject with the following:
  - the identity and the contact details of the controller and, if any, of the controller's representative;
  - the contact details of the Data Controller;
  - 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;

- 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;
- any further information necessary to guarantee fair processing.

- Privacy notice for personal data processing is recorded and all information is provided to the data subject in an easily accessible format via [email], using clear and plain language and/or by directing the data subject to the Association's webpage.
- Insurance Association of Cyprus facilitates the data subject's rights in line with the data protection policy and the subject access request procedure (Section 8.3.1**Error! Reference source not found.**).

7.3.1. Conditions

- Insurance Association of Cyprus provides the information stated in section **Error! Reference source not found.** above within:
  - one month of obtaining the personal data, in accordance with the specific circumstances of the processing;
  - when personal data is first disclosed in circumstances where the personal data is disclosed to another recipient.
- The 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.

8.Data Subjects Rights requests handling procedure

8.1. Scope

- 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 sue for compensation if they suffer damage by any contravention of the GDPR.
  - To take action to rectify, block, erase, including the right to be forgotten, 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;

- Insurance Association of Cyprus is responsible to manage data subject rights requests within the set timeframe.

8.2. Responsibilities

- All Employees are responsible for ensuring any requests or complaints made in relation to the scope of this procedure are reported to Management.

- The Management is responsible for the application and effective working of this procedure The Management is responsible for responding to complaints and Data Subjects Rights Requests, within one month, as per section 8.3. In performing this task the Management may request the assistance of the legal and regulatory affairs asset owner who may prepare a draft reply for Management review and approval. The asset owner who is responsible for the processing activity which is the subject matter of the complaint and/or the Data Subjects Rights Request shall provide his/her full co-operation and assistance in preparing the reply. Any written replies to complaints and Data Subjects Rights Requests shall be signed by the Management representing the Association, the Data Controller. If there are actions that need to be taken, the Management shall then request the asset owners involved to perform any action necessary to comply with the data subject's request in line with the reply of the Association to the data subject and to report back to Management on actions taken.
- An archive will be kept which will also be made available to the supervisory authority.

8.3. Procedure

- A complaint can be submitted in writing to the following e-mail address: info@iac.org.cy
- Once received, the request is immediately forwarded to the Management who may request the assistance of the legal and regulatory affairs asset owner., who will ensure that the request is handled within the specified time frame recorded by the Association following the Association's procedures Any reply to a complaint and/or a Data Subjects Rights Request shall be signed by the Management on behalf of the Association, the Data Controller.
- Insurance Association of Cyprus verifies the individual's identity, in line with the Association's internal procedures.
- Following identification, the corresponding sub-procedure in the following sections will be followed.
- Insurance Association of Cyprus provides an answer 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 or in case of an appeal on the way a request was handled. The Association shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.
- The Association maintains a record of data right requests and of their receipt, including dates and responses.
- Insurance Association of Cyprus responds to requests via email. In case of requests/complaints received in physical form the Association provides a written letter of reply to the contact address given by the data subject.

8.3.1. Data Subject Access Request Sub-Procedure

- Data subjects are entitled to obtain:
  - Confirmation as to whether Insurance Association of Cyprus is processing any personal data about that individual;
  - Access to their personal data;
  - Any related information.
- The data subject specifies to Insurance Association of Cyprus the relevant set of data on their subject access request (SAR). The data subject can request all data held on them.

- Insurance Association of Cyprus records the date that the identification checks were conducted and the specification of the data sought.
- Collection entails:
    - Collecting the data specified by the data subject, or
    - Searching all databases and all relevant filing systems (manual files) in the Association, including all back up and archived files (computerised or manual) and all email folders and archives. Click here to enter text.

  The documents that have been identified as containing information relating to the data subject that submitted the SAR are reviewed to identify whether any third parties are present in it, and if so the identifying third party information is removed from the documentation or the written consent of the third party is obtained for their identity to be revealed.
- In the event that a data subject requests what personal data is being processed then the Insurance Association of Cyprus provides the data subject with the following information:
    - Purpose of the processing
    - Categories of personal data
    - Recipient(s) of the information
    - How long the personal data will be stored for
    - The data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed
    - Inform the data subject of their right to lodge a complaint with the supervisory authority and a method to do so (Complaints Procedure – Section 8.3.2)
    - Information on the source of the personal data if it hasn't been collected from the data subject
    - If and where personal data has been transferred and information on any safeguards in place.

8.3.2. Complaints Sub-Procedure

- This procedure addresses complaints from data subject(s) related to the processing of their personal data, Insurance Association of Cyprus' handling of requests from data subjects, and appeals from data subjects on how complaints have been handled.
- Data subjects are able to complain to the Association 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.
- Complaints are to be resolved within 1 month.
- Appeals on the handling of complaints are to be resolved within 2 months.
- If Insurance Association of Cyprus fails to act on a data subject's request within the appropriate timeframe, or refuses the request, it sets out in clear and plain language the reasons it took no action/refusal.
- Insurance Association of Cyprus will also inform the data subject(s) of their right to complain directly to the supervisory authority. In doing so, Insurance Association of Cyprus provides the data subject(s) with the contact details of the supervisory authority and informs them of their right to seek judicial remedy.

8.3.3. Data Subject Right for Portability Sub-Procedure

- This procedure applies where a data subject exercises their right to data portability and applies to Insurance Association of Cyprus (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 the Association
  - For Insurance Association of Cyprus to transmit the data to another data controller.

Transmitting personal data

- The Management with the assistance of the legal and regulatory affairs asset owner and the IT Security vendor 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.
- Insurance Association of Cyprus 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 structure, commonly used and machine readable format, that allows for the effective re-use of the data.
- When transmitting data to another data controller, Insurance Association of Cyprus forwards the data in an interoperable format. In the event that technical impediments prohibit direct transmission, the Association explains these impediments to the data subject(s).
- The Management with the assistance of the legal and regulatory affairs asset owner and the collaboration and contribution of the responsible for the processing operation asset owner responds to the request, providing details on the actions taken.
- The request does not affect the original retention period that applies to the data that has been transmitted.

Receiving personal data

- Insurance Association of Cyprus 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.
- Insurance Association of Cyprus only accepts and retains data that is necessary and relevant to the service being provided, and provides the data subject with this information**.**
- If data received contains third-party data, the Insurance Association of Cyprus 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 the Insurance Association of Cyprus.

8.3.4. Data Subject Right to be forgotten Sub-Procedure

- Insurance Association of Cyprus complies 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 is withdrawn and there is no other legal basis for the processing;
  - The individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
  - 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 Insurance Association of Cyprus can refuse to deal with a request. Insurance Association of Cyprus can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

  - to comply with a legal obligation for the performance of a public interest task or exercise of official authority
  - the exercise or defence of legal claims;.
  - to comply with any related applicable regulatory requirements.

- Once such a request is received, evaluated and accepted by the Association, the asset owner(s) responsible for the processing activity will ensure that the personal data of the data subject shall be deletedand shall report to Management as to the actions taken.
- Deletion may entail:
  - 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 the Association, including all back up and archived files (computerised or manual) and all email folders and archives.
  - Requesting the deletion and the verification of the deletion of all related data of the data subject from third parties that Insurance Association of Cyprus is associated with.

8.3.5. Data Subject Right to Rectification Sub-Procedure

- Data subjects are entitled to ask for rectification of any personal data submitted to Insurance Association of Cyprus at any given time.
- The data subject identifies the set of data they request to rectify and what rectifications they wish to be made.
- Rectification entails rectifying the data specified by the data subject, in all databases and all relevant filing systems (manual files) of the Insurance Association of Cyprus, including all back up and archived files (computerised or manual) and all email folders and archives.

A response to the request will be provided, outlining the actions taken.

8.3.6. Data Subject Right to restriction of processing Sub-Procedure

- Insurance Association of Cyprus complies with an individual's request for restriction of processing their personal data where one of the following applies:
  - The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.
  - Insurance Association of Cyprus no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.
  - The data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
- The data subject identifies the personal data that they wish to restrict the processing of and provide justification for such request.
- The Management with the assistance of the legal and regulatory affairs asset owner examines if the Right of restriction of processing can be applied. If so, with the exception of storage, the data subject's data can only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.
- The Data Subject is informed that their data has been restricted from processing or alternatively the Data Subject is informed about the reasons why their data cannot be restricted from processing.

- If a data subject has obtained restriction of processing of their personal data, the Association will inform them before the restriction of processing is lifted.

8.3.7. Data Subject right to object Sub-Procedure

- Insurance Association of Cyprus complies with a data subject's objection, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on one of the legal bases of processing of personal data below:
  - official authority of the Association to carry out processing that is in the public interest;
  - the legitimate interests of the data controller or third party.
- The data subject identifies the personal data that they object to the processing of and provide justification for such request.
- Insurance Association of Cyprus examines if the Right to object processing can be applied. If yes, the Insurance Association of Cyprus ceases processing and informs the data subject that their data will no longer be processed and will be destroyed in accordance to the Association's procedures. Alternatively, where the Association demonstrates compelling legitimate grounds for the processing of such data which override the interests, rights and freedoms of the data subject or where such data is required by the Association for the exercise or defence of legal rights/claims the Association shall inform the data subject, following the procedure mentioned above, that the request cannot be satisfied outlining the relevant reasons.

9. Consent Management

- Insurance Association of Cyprus 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.
- For sensitive data, explicit written consent (Consent Procedure – Section 9.1) of data subjects is obtained unless an alternative legitimate basis for processing exists.

9.1. Consent Procedure

9.1.1. Scope

- The consent of the data subject is one of the conditions for the processing of his or her personal data and it is within the scope of this procedure. Insurance Association of Cyprus needs to obtain consent when no other lawful basis applies. Consent is the legal basis for the processing of personal data of data subjects who contact the Association for the provision of information and/or to formulate requests for the transmission of information to the Association members.
- Processing of sensitive personal data is conducted for Association employees to the extent that it is necessary to comply with obligations in the field of employment and social security law as well as to the extent that it is necessary for reasons of public interest in the area of public health.

9.1.2. Responsibilities

- As a data controller, Insurance Association of Cyprus is responsible under the GDPR for obtaining consent from the data subject.

9.1.3. Consent procedure

- Insurance Association of Cyprus provides a clear Privacy Notice wherever personal data is collected (Privacy Notice Document) to ensure that the data subject is informed of their rights in relation to their personal data, including the right to withdraw consent (Right to Withdraw Consent Procedure – Section 9.2).
- Insurance Association of Cyprus ensures that personal data is only processed for the purpose(s) that the data subject has given consent to.
- Insurance Association of Cyprus ensures that consent is:
    - Explicit and only collected for specific purpose(s);
    - 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);
    - Intelligible and accessible using clear and plain language.

9.2. Withdrawal of Consent Procedure

9.2.1. Scope

- 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.

9.2.2. Responsibilities

- As a data controller, Insurance Association of Cyprus, is responsible under the GDPR for administering withdrawal of consent from the data subject.

9.2.3. Withdrawal of consent procedure

- Insurance Association of Cyprus accepts requests in writing for withdrawal of consent for the processing of his or her personal data.
- Where the processing had multiple purposes, Insurance Association of Cyprus demonstrates withdrawal of consent for each purpose as recorded in the request.
- The processing activities that were conducted on the legal basis of consent cease in accordance with the relevant process provided there is no other legal basis for processing the relevant data.

10. Security

10.1. Security of data

- All Employees are responsible for ensuring that any personal data that Insurance Association of Cyprus holds and for which they are responsible, is kept securely.

- Personal data is accessible only to those who need to use it, and access may only be granted in line with this Policy. All personal data is treated with the highest security and is kept:
  - in a lockable room with controlled access; and/or
  - in a locked drawer or filing cabinet; and/or
  - in an electronic form, be password protected in line with corporate requirements and/or
  - stored on (removable) computer media which are encrypted.
- Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of Insurance Association of Cyprus. All Employees are required to enter into an Employment Agreement before they are given access to organisational information of any sort which details rules, on screen time-outs etc.
- Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. Staff must be specifically authorised to process data off-site.
- As soon as manual records are no longer required for day-to-day operations, they are removed from secure archiving.
- Personal data may only be deleted or disposed of in line with the Retention of Data Procedure (Section 14.2).

10.2. Paper and Equipment Security

- Paper based (or similar non-electronic) information are assigned an owner and a classification. If it is considered as sensitive, information security controls to protect it must be put in place.
- All general computer equipment is located in suitable physical locations that:
  - Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration
  - Limit the risk of theft – e.g. if necessary items such as laptops are physically attached to the desk
  - Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.
- Data is stored on network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.
- Business critical systems is protected by an Un-interruptible Power Supply (UPS) to reduce the operating system and data corruption risk from power failures.
- Cables that carry data or support key information services are protected from interception or damage.
- Power cables are separated from network cables to prevent interference. Network cables are protected by conduit and where possible avoid routes through public area.

10.3. Security of personal computers and other relevant equipment

- Computers, laptops and other personal equipment used by personnel are the property of the Association and are given to an employee in order to perform job tasks during the validity period of a job contract between employee and the Association.
- Every employee who receives equipment for use from the Association, is obliged to take appropriate measures to secure it both in the office and on the outside.

10.4. Access to the Internet

- Each employee after the signing of the contract is granted access to the Internet.

- Access to the Internet is used by employees only for execution of immediate work tasks. Any other task maybe executed by employees or guests through access to free Wi-Fi which is not linked to the Association's Network Servers.
- Employees are prohibited from:
    - Publication and distribution of the Association' confidential information and information prohibited by local legislation via the Internet.
    - Publication of text and graphic information (including screenshots) containing the above information on Internet resources.
    - Downloading and launching files that could potentially damage the infrastructure and information systems of the Association.

10.5. Email Use Policy

- Each employee's personal account on mail servers of the Association is password protected.
- Employees are prohibited from:
    - Disclosing confidential information to third parties.
    - Use of corporate mail for transferring and distribution of any information that violates local or international law.
    - Getting access to someone else's mail correspondence or attempting to gain such access.
- If an employee has a suspicion about the content of e-mail message (possible substitution of the sender; suspicious files and links in the message), they immediately notify the IT vendor, in order to prevent attempts to enter the corporate network and compromise confidential information.

11. Disclosure of data

- Insurance Association of Cyprus ensures that personal data is not disclosed to unauthorised third parties.
- All Employees exercise caution when asked to disclose personal data held on another individual to a third party. Disclosure of the information must always be conducted to the extent that it is relevant to and necessary for the execution of Insurance Association of Cyprus' business and/or promotion of the Association's interests.
- All requests to provide data for one of these reasons are supported by appropriate paperwork and all such disclosures are specifically authorised by the Management.

12. Access Right Management and Review

- Formal user access control procedures are documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.
- User access rights are reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts are only be provided to users that are required to perform system administration tasks.

12.1. User Registration and Deregistration

- Access to the organization's network and computer systems is only granted following signing the employment agreement and approved by the Management, who will then request access from IT vendor.
- Each user account will have a unique user name that is not shared with any other user and is associated with a specific individual i.e. not a role or job title.

- An initial strong password is created on account setup and communicated to the user via secure means. The user is required to change the password on first use of the account.
- When an employee leaves the organisation under normal circumstances, their access to computer systems and data is suspended at the close of business on the employee's last working day. It is the responsibility of the Management to request the suspension of the access rights via the IT vendor.
- In exceptional circumstances where there is perceived to be a risk that the employee may take action that may harm the organization prior to or upon termination, a request to remove access may be approved and actioned immediately and in advance of notice of termination being given. This precaution especially applies in the case where the individual concerned has privileged access rights or access to sensitive data.
- User accounts are initially suspended or disabled only and not deleted. User account names are not be reused as this may cause confusion in the event of a later investigation.

12.2. Removal or Adjustment of Access Rights

- Where an adjustment of access rights or permissions is required e.g. due to an individual changing role, this is carried out as part of the role change. It is ensured that access rights no longer required as part of the new role are removed from the user account.
- In the event that a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role is requested. Due consideration of any issues of segregation of duties should be given.
- Under no circumstances are administrators permitted to change their own user accounts or permissions.

12.3. Management of Privileged Access Rights

- Privileged access rights such as those associated with administrator-level accounts are identified for each system or network and tightly controlled. A separate "admin" user account is created and used only when the additional privileges are required by the IT support staff. These accounts are specific to an individual; generic admin accounts are not used as they provide insufficient identification of the user.
- Access to admin level permissions is only allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.

12.4. User Authentication for External Connections

- The use of modems on non-organization owned PCs or devices connected to the organization's network can seriously compromise the security of the network. As such, connecting any non-organisation owned equipment to the organization's network is prohibited.
- Where remote access to the network is required via VPN, a request is made to the Management. Access is granted following his approval and instructions are provided to the IT support accordingly.

12.5. Supplier Remote Access to the Association Network

- Partner agencies or 3rd party suppliers are not be given details of how to access the organization's network without permission from the Management and in accordance to the terms and conditions and data protection safeguards stipulated in the service provision agreements. Any changes to supplier's connections (e.g. on termination of a contract) are immediately processed accordingly so that access can be updated or ceased. All permissions and access methods are controlled by the Management.
- Partners or 3rd party suppliers contact the Management on each occasion to request permission to connect to the network.

12.6. Review of User Access Rights

- Periodically, Management, will review who has access to their areas of responsibility and the level of access in place. This will be done to identify:
  - People who should not have access (e.g. leavers);
  - User accounts with more access than required by the role;
  - User accounts with incorrect role allocations;
  - Any other issues that do not comply with this policy.
- A review of user accounts with privileged access will be carried out by the IT support vendor twice a year to ensure that this policy is being complied with.
- Any corrective actions identified and carried out. Any changes in the roles will immediately be reflected on use accounts and access.

12.7. User Authentication and Password Policy

- Every employee uses strong passwords that meet security requirements. A password is at least 8 characters long and include at least one special character, one number, one uppercase symbol and one lower symbol.
- The password complexity policy described above can be changed in the future with immediate notification of employees about this.
- Employees are prohibited from:
  - Storing any passwords in clear text, including paper-based storage of passwords (organizers etc.) and storage in digital format (documents on personal computers of employees);
  - Transferring any passwords in clear text. This prohibition applies to any method of transferring, including voice, text and digital transfer of data;
  - Transferring their personal passwords to any persons, including other employees of the Association;
  - Using personal identifiers and passwords of other employees of the Association.
- If there is a suspicion of password compromise, the employee immediately notifies the Management and the IT vendor.

13. Information asset register/data inventory

- Insurance Association of Cyprus has established a data inventory and data flow register as part of its approach to address risks and opportunities throughout its GDPR compliance project. Insurance Association of Cyprus' information asset register and data flow register:
  - Determine the business processes that use personal data;
  - Determine the source of personal data;
  - Determine the volume of data subjects;
  - Provide a description of each item of personal data;
  - Detail the processing activity;
  - Include the inventory of data categories of personal data processed;
  - Document the purpose(s) for which each category of personal data is used;
  - Include the recipients, and potential recipients, of the personal data;
  - Demonstrate the role of the Insurance Association of Cyprus throughout the data flow;
  - List key systems and repositories;
  - Cover all data transfers; and
  - Document all retention and disposal requirements.

14. Retention and disposal of records procedure

- Insurance Association of Cyprus 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.
- Insurance Association of Cyprus 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.
- Personal data is 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 (Section 14.3).

14.1. Responsibilities

- Asset owners are responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR.
- The Association is responsible for storage of data in line with this procedure.

14.2. Retention of Data Procedure

- Personal Data of Board of Directors members, Directors, employees, members and vendors that is no longer required because the collaboration with the Association has ceased is erased immediately unless there is an indication and/or the Association receives notice that a legal claim/procedure may or has been initiated.
- The asset owners are responsible for destroying data once it has reached the end of the retention period, subject to Management notification and approval. Destruction is completed within 30 days.

14.3. Disposal of Records Procedure

- Any documents, either electronic or physical, that have reached the end of the set retention period or that are no longer needed, are securely disposed without undue delay.
- Personal data stored on devices that will be re-assigned to other employees is securely deleted before the device is re-assigned.
- If personal data is not securely deleted there is a risk of unauthorised disclosure.

14.3.1. Disposal of information in physical format

- Documents marked as confidential are placed in a shredding bin, until they are collected for shredding.
- The shredding bin is stored in a secure location.
- Documents not marked as confidential are disposed of in the designated recycling bins.

14.3.2. Disposal of information in electronic form

- Information in electronic form is deleted form the systems.
- Redundant IT equipment is wiped and then destroyed or recycled by the IT vendor.

- Asset owners are responsible for notifying the Management who in turn notifies the IT vendor when redundant IT equipment needs to be wiped.
- Redundant IT equipment is securely stored until is collected by the IT vendor.

15. Training Policy/Procedure

15.1. Scope

- This policy applies to Insurance Association of Cyprus' training and awareness programme where relevant to the GDPR, compliance with the GDPR, and other matters relating to data protection and privacy.

15.2. Training Policy/Procedure

- The Management assigns data protection responsibilities to employees/asset owners in relation to Insurance Association of Cyprus' policies and procedures on personal data management.
- Employees are provided with specific training on processing personal data relevant to their individual day-to-day roles and responsibilities, and in accordance with Insurance Association of Cyprus' policies and procedures.
- It is the responsibility of each asset owner in carrying out their day-to-day responsibilities involving personal data and processing operations, and those with permanent/regular access to personal data, to demonstrate compliance with the GDPR and understand the importance of data protection.
- The Management and the asset owner responsible for human resources issues ensure that the employees are kept up to date and informed of any issues related to personal data, and that all security requirements related to data protection are communicated to them.
- All Employees involved in personal data processing will at planned intervals assess the capability of any systems used to record personnel information, to demonstrate compliance to the GDPR.
- The Management with the assistance of the asset owner responsible for human resources issues shall promote training and awareness programmes, and the Insurance Association of Cyprus shall make resources available in order to raise awareness.
- The asset owner responsible for human resources issues, acting on the instructions of Management is responsible for organising relevant training for all responsible individuals and Employees generally, and for maintaining records of the attendance of staff at relevant training at appropriate times across Insurance Association of Cyprus' business cycle.

16. Data Protection Impact Assessment procedure

16.1. Scope

- All 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).

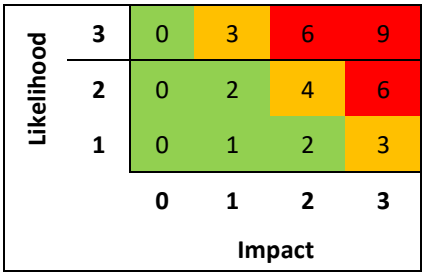
16.2. Responsibilities

- The Management is responsible for assessing the need for conducting a DPIA. Indicatively such a need will arise if the Association undertakes a new role that involves processing of personal data and/or expands its activities and or services to its members.
- In fulfilling this obligation the Management may request the assistance of the Statistics asset owner along with the asset owner(s) responsible or involved with the processing activity who will prepare a DPIA who will be reviewed, approved and signed by the Management.
- The Management and responsible asset owners are responsible for ensuring that appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.
- The Association's employees are responsible for implementing any privacy risk solutions identified.

16.3. Procedure

- Insurance Association of Cyprus 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, Insurance Association of Cyprus 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

16.4. Data processing workbook (Data Flow)

- Insurance Association of Cyprus records key information about all personal data processed for each project, activity, technology, software etc This includes a description of the processing and purposes; legitimate interests pursued by the controller; an assessment of the necessity and proportionality of the processing; an

assessment of the risks to the rights and freedoms of data subjects (as per the matrix and risk level definitions in section 16.3 above).

- Insurance Association of Cyprus captures the type of processing activity associated with the personal data being processed as part of the project. These are categorised as:
  - Collection
  - Transmission
  - Storage
  - Access
  - Deletion
- Insurance Association of Cyprus establishes on what lawful basis the data is being processed and its appropriate retention period (in line with Retention of Data Procedure – Section 14).
- Insurance Association of Cyprus identifies the category of data processed, whether it is personal, special or that of a child's, and the format of the data.
- Insurance Association of Cyprus identifies who has access to the data (individuals, teams, third-parties or data processor) or who are involved in the processing of personal data, or processing activity, recording the geographic location of where the processing takes place and / or if it is transborder processing.

16.5. Identify privacy risks

- Insurance Association of Cyprus assesses the privacy risks for each process activity as described in section 16.3 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, the Association 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).
- Insurance Association of Cyprus identifies solutions to privacy risks, assigns a risk treatment owner and sets a target date for completion.
- Insurance Association of Cyprus prioritises analysed risks for risk treatment based on the risk level criteria established in section 16.3 above.
- The Management in consultation with the Insurance Association of Cyprus risk owner(s), approves and signs off each DPIA for each data processing activity.

16.6. Prior consultation (Article 36, GDPR)

- Where the DPIA identifies that processing of personal data will result in high risk to the data subject, in the absence of risk mitigating measures and controls, the Association consults with the supervisory authority, using the following method.
- When Insurance Association of Cyprus requests consultation from the supervisory authority it provides the following information:
  - details of the responsibilities of the Association as the controller requesting the authorisation to process personal data and any other processors/joint controller involved in the processing;
  - purpose of the intended processing;

- detail of any/all measures and controls in place/provided to protect the rights and freedoms of the data subject(s);
- contact details of the Management and the responsible risk owner(s);
    - a copy of the data protection impact assessment; and
    - any other information requested by the supervisory authority.

17. Regulatory Interventions Procedure

- Response to regulatory interventions by the supervisory authority is managed by the Management who may request the assistance or may appoint the legal and regulatory affairs asset owner to act as liaison between the regulatory authority and the Association. The response of the Association to regulatory interventions will be based on a clear and established procedure. This procedure among others, may 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 organisation.
    - 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.
    - Ongoing communication and liaison with the supervisor.
    - Collation of evidence and responses to regulatory intervention in a formal deliverable to be handed to the supervisory authority.

18. Breach Detection and Response

- Security incidents have the potential to disrupt business operations by undermining the confidentiality, integrity and availability of data assets foundational to the provision and support of key business processes. Minimizing the destructive potential of incidents requires the development of a solid attack detection and response capability and the adoption of processes to support that.
- A solid attack detection capability relies on:
    - Well-architected, properly configured, diligently patched and regularly tested perimeter and internal defences.
    - The continuous logging and monitoring of activity on systems and networks, and its regular evaluation.
    - Employees being educated to detect and empowered to report any suspicious activity they spot on the systems and networks within which they operate.
    - Clearly defined reporting frameworks covering points of contact and escalation in cases of suspected incidents.
- A solid attack response capability relies on:
    - The above being in place.
    - Clearly defined and communicated roles and responsibilities.
    - Tried and tested frameworks for the effective and swift response to incidents.

18.1. Scope

- This procedure focuses on a specific type of information security incidents namely: ‘Data Breaches’. A ‘Data Breach’ is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorised party.

- Data Breaches should be treated in the same way as other types of incident.
- Insurance Association of Cyprus is responsible to manage this kind of incidents, for its personal data processing activities.

18.2. Responsibilities

- The Management, in collaboration with the IT vendor, is responsible for the management of data breaches incidents.

18.3. Procedure

18.3.1. Incident Management – Data Breaches

- For the purpose of this procedure, data breaches include both confirmed and suspected incidents.
- For all data breaches the 'Incident Handling' process is followed. This means that:
    - An Incident record is created;
    - The Management co-ordinates resolution and communications, in collaboration with the implicated service providers as applicable;
    - An Incident Report is produced after the incident is resolved, detailing the cause, lessons learned etc.
- Due to the varied nature of information security incidents, a number of additional steps may be required in order to manage the incident effectively.

18.3.2. Contain the Incident

- In the first instance, the IT Security Officer asset owner and/or any internal asset owner who may be designated by Management (where applicable depending on the processing operation and the data affected by the breach) shall establish whether the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.
- An initial assessment will be made by the responsible asset owners in liaison with relevant staff to establish the severity of the breach and report back to Management who will decide who will take the lead investigating the breach on the Management's behalf.
- Once the incident has been confirmed and an initial hypothesis and understanding of the nature of the incident has been established, a containment strategy is developed, to ensure the incident severity does not get exacerbated, while it is being under further investigation. Incident containment depends entirely on the type of incident being managed and could include actions such as blocking domains, removing hosts from the network, isolating devices from the network, blocking a user account etc.

18.3.3. Eradicate and Recover

- Once a clear picture of what has happened is established, the asset owner who is in charge of the investigation coordinates an eradication and recovery process to ensure all traces from activity related to the incident are removed from the system before the system can resume its normal operations.
- Any actions to eradicate damage and recover information affected by the incident aims to fix the current cause and prevent the incident from re-occurring.
- Any actions to eradicate damage and ensure all traces of activity related to the incident are removed, are verified and confirmed to be effective.

18.3.4. Evidence Gathering

- In the course of an incident being handled accurate records mush be kept of all actions taken and all evidence gathered. This information will be relevant for further incident investigation.
- This may include:
  - Screen shots of relevant messages or information
  - Audit logs
  - Manual records of the chronology of the incident
  - Original documents, including records of who found them, where and when
  - Details of any witnesses
- Once collected, the evidence is kept in a safe place where it cannot be tampered with.
- The evidence may be required:
  - For later analysis as to the cause of the incident
  - As forensic evidence for criminal or civil court proceedings
  - In support of any compensation negotiations with software or service suppliers.

18.3.5. Inform the Relevant Authorities

- In the event, the type of incident (e.g. personal data breach) warrants special notification requirements (e.g. reporting to the commissioner), the timelines imposed by law/industry must be adhered to.
- In the event that the evidence points to a deliberate act, the IT vendor (Information Security Officer assigned to the Association) and the internal asset owner (if applicable) in coordination with the Management and the legal and regulatory affairs asset owner decide whether it is appropriate to contact the relevant authorities such as the Commissioner for the Protection of Personal Data, the Police as well as affected parties. Any written communication with competent and/or law enforcement authorities and affected data subjects shall be signed by the Management.

19. Personal Data Breach Notification procedure

19.1. Scope

- 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 supervisory 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 recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation establishes whether it is a data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

19.2. Responsibility

- All users (whether employees, contractors or temporary employees and third party users) and owners of Insurance Association of Cyprus are required to be aware of, and to follow this procedure in the event of a personal data breach (reference Training Policy – Section 15).
- All employees, contractors or temporary personnel are responsible for reporting any personal data breach to the Management.

19.3. Procedure – Breach notification data controller to supervisory authority

- Insurance Association of Cyprus determines if the supervisory authority needs to be notified in the event of a breach.
- Insurance Association of Cyprus 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 a data protection impact assessment against the breach and/or other means available.
- If a risk to data subject(s) is likely, the Association reports the personal data breach to the supervisory authority without undue delay and where feasible, not later than 72 hours.
- If the data breach notification to the supervisory authority is not made within 72 hours, the Insurance Association of Cyprus submits it electronically with a justification for the delay.
- If it is not possible to provide all of the necessary information at the same time, the Association will provide the information in phases without undue further delay.
- The following information needs to be provided to the supervisory 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 Association's Management.
  - Consequences of the breach.
  - Any measures taken to address the breach.
  - Any information relating to the data breach.
- The Association's Management notifies the supervisory authority.
- The breach notification is provided in writing.
- A confirmation of receipt of this information is provided in writing.

19.4. 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, Insurance Association of Cyprus notifies the data subjects affected immediately.
- The notification to the data subject describes the breach in clear and plain language, as specified in section 214.2.
- Insurance Association of Cyprus takes measures to render the personal data unusable to any person who is not authorised to access it. Insurance Association of Cyprus 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, Insurance Association of Cyprus makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder the Insurance Association of Cyprus' 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 Insurance Association of Cyprus has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Insurance Association of Cyprus will communicate the data breach to the data subject within 48 hours.
- Insurance Association of Cyprus documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

20. Risk Assessment and treatment procedure

20.1. Identification of Risks

- The process of identifying risks will consist of the following steps in line with the requirements of best practise and industry standards. Risks are identified to the confidentiality, integrity or availability of information.

20.2. Identify Potential Threats

- For each asset, the threats that could be reasonably expected to apply to it will be identified. These will vary according to the type of asset and could be accidental events such as fire, flood or vehicle impact or malicious attacks such as viruses, theft or sabotage.

20.3. Assess Existing Vulnerabilities

- Circumstances or attributes of an asset which may be capitalised on by any specific threat will be detailed. Examples of such vulnerabilities may include a lack of patching on servers (which could be exploited by the threat of malware) or the existence of paper files in a data centre (which could be exploited by the threat of fire).

20.4. Assess the Likelihood

- An estimate of the likelihood of the threat occurring is made. This takes into account whether it has happened before either to this organization or similar organizations in the same industry or location and whether there exists sufficient motive, opportunity and capability for the threat to become real.

20.5. Assess the Impact

- Finally an estimate of the impact that the loss of confidentiality, integrity or availability of the asset could have on the organization is given.
- Consideration is given to the impact in the following areas:
  - Finance
  - Health and Safety
  - Reputation
  - Knock-on impact within the organization
  - Legal, contractual or organizational obligations

21. Review of this Policy

- This Policy will be reviewed annually and/or as and when necessary to be amended by the Management with the assistance of the legal and regulatory affairs asset owner in consultation with the internal asset owners as well as the IT vendor. The Board of Directors shall approve any amendments to this Policy.
- A current version of this document is available to all members of staff.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	<>	Xx/yy/zz