Document ID	Document Name	Document Classification	Version	Date
GP_GDP_COM01	Data Protection Policy	Internal	V 1.0	26-Apr-18

Revision History [SEPG]

Srl. No.	Version No.	Author/Owner	Date of Release	Description of Release/Change	Approved By
1.	1.0	Anand Kapoor	26-Apr-2018	Initial Release	EVP

Table of Contents

1. GDPR Background

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 'living individuals' and to ensure that personal data is processed with their consent and not processed without their knowledge.

2. Definitions

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

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 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.

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.

3. Policy Statement

"Pyramid is committed to document its business activities with records that are complete, authentic, reliable, secure and accessible and comply with data protection requirements of EU GDPR throughout their lifecycle, from planning and creation to ultimate disposal. It also ensures to comply with all data protection principles".

In view of the policy, the top management of Pyramid is committed and will ensure the following:

- The personal information obtained will be processed fairly, supported by a legal basis and used in a transparent manner, respecting the data subjects' rights and will not be processed unless the processing is necessary for the purposes defined under the EU General Data Protection Regulation.
- The information obtained will be:
    - Adequate, relevant and not excessive for the purposes.
    - Accurate and kept up to date.
    - Kept for no longer than is necessary for the purpose and disposed timely and appropriately.
    - Processed in accordance with the data subject's rights.
    - Kept secure from unauthorized access, accidental loss or destruction.
    - Transferred to a country outside the European Economic Area (EEA) under circumstances where the personal information can be adequately protected.
- The personal information under its control is managed in compliance with the EU General Data Protection Regulation.
- Procedures are in place to enable the rights of individuals to be respected.
- Establish a governance framework to implement, and monitor this policy.
- Provide clear guidance for employees and external agencies, working on behalf of Pyramid to help them to use and share personal information securely and in full compliance with EU General Data Protection Regulation.
- Ensure that disclosures to third parties are managed in compliance with EU General Data Protection Regulation.
- Ensure that personal information processed by third parties on behalf of Pyramid is managed in compliance with EU General Data Protection Regulation.
- Ensure that the level of security imposed to ensure compliance and protect individual rights will not prevent access to information where this is a legal or reporting requirement.
- Ensure the awareness of Privacy through on ongoing education and training programs.
- Implement measures to ensure privacy by design and default, wherever applicable, such as Data minimization, Pseudonymization, and Anonymization.

- Ensure the responsibility and accountability to relevant people throughout the organization and ensure communication of this policy.
- Manage the data protection risks by identifying, evaluating and mitigating.
- Continually improve the personal information management system through privacy enhancing innovations.

4. Roles and Responsibilities under GDPR

Top Management and all those in senior managerial role at Pyramid are responsible for sponsoring & approving funds required for GDPR implementation, Approving data protection/privacy policy and its objectives, Ensuring that compliance with data protection legislation under the DPA, EU GDPR, any other data protection legislation and good practice can be demonstrated as defined in document 'Roles and Responsibilities'

Since none of the data processing at Pyramid is being done under article 37.1 the designation of Data Protection Officer is not mandatory. However, **Anand Kapoor** (email: anand.kapoor@pyramidci.com) has been appointed as Data Protection Officer/GDPR owner and is responsible for compliance under GDPR.

Data Protection Officer/GDPR owner is responsible for single point of contact for GDPR related activities, ensuring implementation of the data protection policy, training and ongoing awareness as required by the data protection policy etc. as defined in document 'Roles and Responsibilities'.

Internal Auditor is responsible for making judgment on the effectiveness of the data protection/privacy policies, procedures etc., reporting internal audit findings to the top management/DPO and recommending the corrective measures etc. as defined in document 'Roles and Responsibilities'.

Employees are responsible for ensuring that they comply with data protection/privacy policy and its objectives, adheres to data protection/privacy policy directions such as consent management, document retention, detection of data breach and breach notification etc. as defined in document 'Roles and Responsibilities.

References

FR_GDP_COM15-Roles & Responsibilities

5. Data protection principles

All processing of personal data at Pyramid is conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Pyramid policies and procedures are designed to ensure compliance with the 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 processor has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

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

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

- Identity and the contact details of the processor and/or processor's representative.
- Contact details of the Data Protection Officer or similar role.
- Purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
- Period for which the personal data will be stored.
- Existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions relating to exercising these rights, such as whether the lawfulness of previous processing will be affected.
- Categories of personal data concerned (*Note: This is not applicable as per GDPR article 30, because the no of consultants placed by Pyramid are less than 250*).
- Recipients or categories of recipients of the personal data, where applicable (*Note: This is not applicable as per GDPR article 30, because the no of consultants placed by Pyramid are less than 250*).
- Where applicable, that the processor 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.

Personal data can only be collected for specific, explicit and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of GDPR register of processing. This is defined in 'PIM Policy'.

Personal data must be adequate, relevant and limited to what is necessary for processing (Data Minimization).

- The Data Protection Officer/GDPR owner is responsible for ensuring that Pyramid does not collect information that is not required for the purpose for which it is obtained.
- All data collection forms (electronic or paper-based), including data collection requirements include a Data Protection Policy or link to Data Protection Policy and approved by the Data Protection Officer.
- Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit or external experts to ensure that collected data continues to be adequate, relevant and not excessive.
- Data Protection Officer is responsible to ensure that Personal data is accurate and kept up to date with every effort to erase or rectify without delay.
- Data that is stored by the data processor must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
- Ensure that all employees 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 Pyramid is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.
- Employees/Clients/Vendors should be required to notify Pyramid of any changes in circumstance to enable personal records to be updated accordingly as defined in procedure 'PR_GDP_COM05-GDP'. It is the responsibility of Pyramid to ensure that any notification regarding change of circumstances is recorded and acted upon.
- The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
- Data Protection Officer will review the retention dates of all the personal data processed by Pyramid, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose as defined in 'Document Retention Policy'. This data will be securely deleted/destroyed in line with the Secure Disposal as defined in 'Data & Media Handling Policy'.

- The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month as defined in procedure 'PR_GDP_COM05-GDP'. This can be extended to a further two months for complex requests. If Pyramid decides not to comply with the request, the Data Protection Officer/GDPR Owner must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.
- The Data Protection Officer/GDPR Owner 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.

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

- Where personal data is retained beyond the processing date, it will be [minimised/encrypted/pseudonymised] in order to protect the identity of the data subject in the event of a data breach as defined in procedure 'PR_GDP_COM05-GDP'.
- Personal data is to be retained as defined in 'Document Retention Policy' and, once its retention date is passed, it must be securely destroyed as defined in 'Data & Media Handling Policy'.
- The Data Protection Officer/GDPR Owner must specifically approve any data retention that exceeds the retention periods defined in 'Document Retention Policy', and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation..

Personal data must be processed in a manner that ensures the appropriate security. The Data Protection Officer/GDPR Owner will carry out a risk assessment taking into account all the circumstances of Pyramid's controlling or processing operations.

In determining appropriateness, the Data Protection Officer/GDPR Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. employees or customers) if a security breach occurs, the effect of any security breach on Pyramid itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical and organizational measures, the Data Protection Officer/GDPR Owner will consider the following:

- Password protection as defined in 'Password Security Policy'.
- Automatic locking of idle terminals as defined in 'Acceptable Usage Policy'.
- Removal of access rights for USB and other memory media as defined in 'Access Control Policy' and procedure 'Systems Administration'.
- Virus checking software and firewalls as defined in 'Firewall Management Policy', and procedure 'Systems Administration'.
- Role-based access rights including those assigned to temporary staff as defined in procedure 'Systems Administration'.
- Encryption of devices that employees take them along while going home such as laptops as defined in 'Encryption Policy' and procedure 'Systems Administration'.
- Security of local and wide area networks as defined in procedure 'Systems Administration'.
- Privacy enhancing technologies such as pseudonymization and anonymization.
- Identifying appropriate international security standards relevant to Pyramid.
- Regular training sessions and awareness workshops to relevant employees.
- Measures that consider the reliability of employees (e.g. Background Verification).
- The inclusion of data protection clauses in employment contracts.
- Identification of disciplinary measures for data breaches.
- Monitoring of employees for compliance with relevant security standards.
- Physical access controls to electronic and paper-based records.
- Adoption of a clear desk policy as defined in 'Acceptable Usage Policy'.
- Storing of paper-based data in lockable cabinets as defined in 'Acceptable Usage Policy'.
- Restricting the use of portable electronic devices outside of the workplace.
- Prohibiting the use of employee's own personal devices being used in the workplace as defined in 'Acceptable Usage Policy'.
- Strictly following clear rules about passwords as defined in 'Password Security Policy'.

- Making regular backups of personal data and storing the media in a secure place. As defined in 'Backup Policy'.

The above mentioned 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. Pyramid's compliance with this principle is contained in its Information Security Management System (ISMS), which is already in practice since year 2012 in line with ISO/IEC 27001 and the information security policy as defined in 'Information Security Policy'.

Pyramid must be able to demonstrate compliance with the GDPR's other principles (accountability)
The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires Pyramid to demonstrate that we comply with the principles and states explicitly that this is our responsibility.

Pyramid 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, risk assessment, breach notification procedures and incident response plans.

References

GP-GDP_COM03-PIM Policy

SP_SEC_COM02-Information Security Policy

SP_SEC_COM20-Data & Media Handling Policy

SP_SEC_COM05-Acceptable Usage Policy

SP_SEC_COM18-Password Security Policy

SP_SEC_COM07-Document Retention Policy

SP_SEC_COM25-Access Control Policy

SP_SEC_COM45-Firewall Management Policy

SP_SEC_COM27-Encryption Policy

PR_SUP_COM25-System Administration

6. Data Subject 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.
- Prevent processing, which is likely to cause damage or distress.
- Prevent processing for purposes of direct marketing.
- Be informed about the mechanics of automated decision-taking process that will significantly affect them.
- Sue for compensation if they suffer damage by any contravention of the GDPR.
- Take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- Request the supervisory authority to assess whether any provision of the GDPR has been contravened.

- Personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another processor or controller.
- Object to any automated profiling that is occurring without consent.
- Make data access requests.
- Complain to Pyramid at supportgdpr@pyramidci.com related to the processing of their personal data, and appeal on how complaints have been handled.

7. Consent Management

Pyramid understands that **'Consent'** is explicitly and freely given. Consent is specific, informed and unambiguous indication of the data subject's wishes by statement or by a clear affirmative action. It signifies agreement to the processing of personal data relating to data subject. The data subject can withdraw their consent at any time.

Pyramid understands that 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.

The basis of Consent is the active communication between the parties. Consent cannot be inferred from non-response to a communication. It is the responsibility of the processor to demonstrate that consent was obtained for the processing operation.

Pyramid has to obtain explicit written consent for sensitive data of data subjects as defined in procedure 'PR_GDP_COM05-GDP'.

In most instances, consent to process personal and sensitive data is obtained routinely by Pyramid using Consent Form.

Pyramid is not providing the services to children as of now. The GDPR clause related to children is Not Applicable.

References

PR_GDP_COM05-GDP

FR_GDP_COM05-Consent Form

8. Security of Data

All Employees are responsible for ensuring that any personal data is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorized by Pyramid to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security and must be kept:

- Under lock in a locked drawer or filing cabinet (Physical documents)
- Under password protected as defined in 'Access Control Policy'.
- Stored on (removable) computer media which are encrypted as defined in 'Data & Media Handling Policy'.

Care must be taken to ensure that Laptop and PC screens are not visible except to authorized employees of the division. All Employees are required to sign the 'Acceptable Usage Policy' before they are given access to organizational information.

Manual records may not be left where they can be accessed by unauthorized personnel and may not be removed from business premises without written authorization. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

Personal data may only be deleted or disposed of in line with the 'Document Retention Policy'. Manual records that have completed their retention period are to be shredded and disposed-off. Hard drives of redundant PCs are to be removed and immediately destroyed as defined in 'Data & Media Handling Policy'.

References

SP_SEC_COM25-Access Control Policy

SP_SEC_COM20-Data & Media Handling Policy

SP_SEC_COM05-Acceptable Usage Policy

SP_SEC_COM07-Document Retention Policy

9. Disclosure of Data

Pyramid ensures that personal data is not disclosed to any unauthorized persons (e.g. family members, friends, government bodies, police etc.). All Employees exercise caution when asked to disclose personal data of data subjects to a third party. The regular awareness sessions conducted for the employees of the respective division helps them to deal effectively with any such risk associated with disclosure of data. All requests to provide data for disclosures are routed to Data Protection Officer (DPO) for action.

10. Retention and Disposal of Data

Pyramid will not keep personal data in a form that permits identification of data subjects and for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

Pyramid may store data for longer periods if the personal data is 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.

The retention period for personal data is defined in 'Document Retention Policy' along with the statutory obligations Pyramid has to retain the data.

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 'Data & Media Handling Policy'.

References

SP_SEC_COM20-Data & Media Handling Policy

SP_SEC_COM07-Document Retention Policy

11. Data Transfer

All imports of data from within the European Economic Area (EEA) to Pyramid (referred to in the GDPR as 'third countries') are received as defined in 'Information Transfer Policy'.

References

SP_SEC_COM30-Information Transfer Policy

12. Personnel Data Inventory

Pyramid has established a data inventory as part of its approach to address risks and opportunities throughout its GDPR life-cycle. The data inventory includes:

- Business process that use personal data.
- Source of personal data.
- Volume of data subjects.
- Description of each item of personal data.
- Processing activity.
- Inventory of data categories of personal data processed, if applicable.
- Documents the purpose(s) for which each category of personal data is used, if applicable.
- Recipients, and potential recipients, of the personal data, if applicable.
- key systems and repositories;
- Data transfer details.
- Document retention requirements and disposal.

Pyramid is aware of any risks associated with the processing of particular types of personal data.

Pyramid assesses the level of risk to data subjects associated with the processing of their personal data. Risk assessment are carried out in relation to the processing of personal data by Pyramid, and in relation to processing undertaken by other parties on behalf of Pyramid in order to reduce the likelihood of a data breach.

Pyramid carry out a risk assessment to find out the impact on the processing operations on the protection of personal data, where new technologies are used, resulting into high risk to the rights and freedoms of data subjects.

The Data Protection Officer may escalate the matter to the supervisory authority, if it notices that processing of personal data using new technologies could cause damage and/or distress to the data subjects.

Pyramid is certified for ISO 27001 and maintain this status since year 2012. In view of this, Pyramid will leverage the best practices of ISO 27001 controls and will apply to reduce the level of risk associated with processing of personal data to an acceptable level.

References

FR_SEC_COM27-Risk Assessment