Data Protection Policy

Version 1.2

Document History

Document Version	Date	Author	Reviewed by	Approved by	Remarks
0.1	24th March 2017	Consultant			Draft
1.0	27th March 2017		Director	Director	Reviewed
1.0	30th July 2018		Parvati	Ravisha TC	Reviewed but no changes done
1.0	11th May 2019		Parvati	Ravisha TC	Reviewed but no changes done
1.0	03rd June 2020		Prathibha SH	Ravisha TC	Reviewed but no changes done
1.1	4th June 2021		Prathibha SH	Ravisha TC	Added Section 19
1.2	10th June 2022		Prathibha SH	Ravisha TC	Updated section 19

1. INTRODUCTION

This document sets out the obligations of PearlArc Systems Pvt Ltd. (here after referred as "PearlArc") with regard to data protection and the rights of people with whom it works in respect of their personal data under the Data Protection Act 1998 ("the Act").

This Policy shall set out procedures which are to be followed when dealing with personal data. The procedures set out herein must be followed by the Company, its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company.

The Company views the correct and lawful handling of personal data as key to its success and dealings with third parties. The Company shall ensure that it handles all personal data correctly and lawfully.
to safeguard processing of personal data by means of appropriate technical and organisational measures and, where possible, to anonymise or pseudonymise personal data. All measures implemented must take the risk associated with the respective data processing operation into consideration and be state of the art. In particular, the effectiveness of the measure should take account of the protection objectives of confidentiality, availability, integrity and capacity. This is supported by integrating data protection measures, information security and additional measures to safeguard data processing operations.
Definition of security value terms:
• **Confidentiality**: Protection of data, information and programmes against unauthorised access and disclosure.
• **Integrity**: Factual and technical accuracy and completeness of all information and data during processing.
• **Availability**: Information, data, applications, IT systems and IT networks are available for processing.
• **Quality**: Denoted as an aspect of availability and thus the capacity of information, data, applications, IT systems and IT networks in the event of malfunction, failure or heavy use.

2. SCOPE AND APPLICABILITY

This Policy applies to all employees and internal consultants/temporary personnel resources of the PearlArc, including all of its wholly owned subsidiaries. The Policy also governs data relating to customers, partners, suppliers and shareholders.

3. ABBREVIATION

IMSO –Integrated Management System Officer

4. POLICY STATEMENT

- Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information and we recognize the need to treat it in an appropriate and lawful manner.
- The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, Distributors and customers and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

- This policy does not form part of any employee's contract of employment and it may be amended at any time. However, any breach of this policy will be taken seriously and may result in disciplinary action.

5. STATUS OF THE POLICY

This policy has been approved by the Board of Directors of PearlArc. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

6. DEFINITION OF DATA PROTECTION TERMS

- Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.
- Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal data.
- Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).
- Data Controllers are the people who or organizations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. PearlArc is the Data Controller of all personal data used in its business and in that of its subsidiary companies.
- Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.
- Data processors include any person who processes personal data on behalf of a Data Controller. Employees of Data Controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.
- Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
- Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

7. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.

- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organizations situated in countries without adequate protection.

8. FAIR AND LAWFUL PROCESSING

- The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the Data Controller is; who the Data Controller's representative is (in this case the Company Secretary; the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.
- For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the Data Controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

9. PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

10. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

11. ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

12. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Company Secretary.

13. PROCESSING IN LINE WITH DATA SUBJECTS RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a Data Controller.

- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Access control/User control

- It must be ensured that authorised persons can only access the data covered by their access authorisation when using a data processing system and that personal data are not read, copied, altered or deleted without authorisation when processing, using and after storing personal data. This is done by:

Authorisation concept

- Rules are established for granting and managing access authorisation.
- Individual access rights and user groups have been formed.
- User groups are managed in a Active directory service.
- Granted authorisation is regularly reviewed.

Access control

- Network access security has been set up.
- Only approved hardware and software are used.
- Network components are protected.
- The network is segmented
- Critical services are subject to monitoring.
- The secure disposal of information is maintained .

Safekeeping when using data storage devices

- Hard drives are hardware encrypted.

Regulation concerning storage on removable media

- In principle, private data storage devices are prohibited on business premises; case-specific exceptions are only approved on request.

Creation and safekeeping of backups

- A documented data backup concept is available.
- Controlled and regular backup of files
- Testing of data backup is regularly carried out and documented.
- Data backup is protected against unauthorised access.
- Backup disks are securely stored separately from the original data at specially protected locations.

Internet connection

- A redundant internet connection is available.
- Also we have backup internet connection

Uninterruptible power supply

- An uninterruptible power supply (UPS) with sufficient capacity is installed upstream of the data centre.
- Proper functioning is ensured by means of regular testing.
- Tests are documented.

Fire protection

- CO2 handheld fire extinguishers are available in the office premises.

Measures for operational disaster control

- A Disaster Recovery Manual (with responsibilities) has been prepared and is maintained.
- Emergency organisation is in place.
- Emergency drills are carried out and documented.

14. DATA SECURITY

- We must ensure that appropriate security measures are taken against unlawful or unauthorized processing of personal data, and against the accidental loss of, or damage to personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.
- The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.
- Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

  - Confidentiality means that only people who are authorized to use the data can access it.

  - Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

  - Availability means that authorized users should be able to access the data if they need it for authorized purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

  - Quality means an aspect of availability and thus the capacity of information, data, applications, IT systems and IT networks in the event of malfunction, failure or heavy use.

15. SECURITY PROCEDURES INCLUDE

- Entry controls. Any stranger seen in entry-controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal. Paper documents should be shredded. CD-ROMs should be physically destroyed when they are no longer required.

- Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

16. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to [their line manager OR the Data Protection Compliance Manager] immediately.

17. PROVIDING INFORMATION OVER THE TELEPHONING

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Refer to [their line manager OR the Data Protection Compliance Manager] for assistance in difficult situations. No-one should be bullied into disclosing personal information.

18. PENALTIES AND CONSEQUENCES

Breaches of the Company's commitment to carefully protect PearlArc Confidential information can have serious repercussions on many levels, as well as damage the Company's reputation. Potential violations will be subject to investigation by the Company and/or its agents, and any failure to comply with this Policy may result in discipline, up to and including termination, referral to regulatory authorities, and potential civil and criminal exposure.

19. REFERENCE

- ISO 27001: A.7.3.1 Termination Or Change Of Employment Responsibilities
- ISO 27001: A.8.3.3 Physical Media Transfer
- ISO 27001: A.9.2.4 Management Of Secret Authentication Information Of Users
- ISO 27001: A.11.1.5 Working In Secure Areas
- ISO 27001: A.13.2.1 Information Transfer Policies & Procedures
- ISO 27001: A.13.2.4 Confidentiality Or Non-Disclosure Agreements
- ISO 27001: A.14.1.2 Securing Application Services On Public Networks
- ISO 27001: A.18.1.2 Intellectual Property Rights