Data Protection Policy

Pre-Pay Electronic Payments Ltd

1. Introduction

It is the policy of Pre- Pay Electronic Payments Ltd (hereinafter: ”Pre-Pay”) to take all the necessary precautions to insure the protection of its customer’s information.

The access and management of the information is granted under a strict authorization system solely to our company employees and our processing partners.

The company’s personnel are being constantly guided and briefed on the subject. Customer information is not to be transferred to a third party unless it is necessary for processing requirements or legal and regulatory obligations.

Pre-Pay will apply procedures to protect its customers from unauthorized access to or unauthorized alteration, disclosure or destruction of information it holds. The company is implementing safeguards that protect the information against illegitimate use. The also follows best practices for information security including continuous reviews of our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems. When processing personal information, our employees must abide by strict data processing guidelines based on applicable law and may be disciplined or terminated if they fail to meet these obligations.

2. Legal Framework

The Company will operate in accordance with the laws, orders, provisions, requirements and directives set forth hereafter:

Protection of Privacy Law (5741-1981) (PPL)

3. Policy statement

The company will provide adequate safeguards to ensure that personal information is protected to prevent unauthorized access & use of both physical & electronic data. To mitigate risks related to cyber security the company will install and maintain appropriate data protection systems such as antivirus and firewall systems. The company will provide a secured physical environment to its branches including closed circuit cameras.

4. Data protection officer

Data protection office will be nominated by the company CEO, his responsibilities will include:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on tricky Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

5. Employee training

All employees will be trained regarding the following data protection related guidelines:

- All employees will receive a unique PIN.
- All PIN's must be personal and will not be used by multiple employees.
- The PIN will not be posted at the agent location or in customer.
- All computers will be logged/turned off when not in use.
- Computers used for processing transaction will not be used for checking e-mail or browsing the internet or online banking.
- No customer information will be released to a third party including spouse or family member unless the request is made by a court order or from a government authority

- No information about his/her activity will be provided to the customer without verifying and authenticating his/her identity.

6. Registration of database

Pre-Pay will register its databases with the Registrar of Databases (Registrar) when any of the following is true:

- The number of data subjects in the database exceeds 10,000.
- The database includes personal information that was not provided
- by the data subjects, on their behalf or with their consent.
- The database is used to provide direct mailing services to others.

7. Fair processing

All personal data will be processed fairly and lawfully, with appropriate notice provided and in line with the expectations of the relevant data subjects.

When collecting personal information from customers a consent to store and handle the information will be obtained from the data subjects at the time of the data collection. This can be done by means of a privacy notice.

8. Data Security

The company will ensure that the personal data is stored and handled in line with information security policies and processes.

Ensure that organization measures are in place to guard against unauthorized or unlawful damage or destruction of the personal data. Such measures could include: restricting physical and computer-based access to the data, ensuring that all digital personal data is password protected, ensuring that any personal data are not left 'in the open' either in paper form, or on a screen in digital form, minimize the need for transfer of the data.

Pre-Pay will take steps to provide an adequate level of training is provided to anyone with access to the personal data, inclusive of anyone outside of the company that may have access to the data. The company will ensure that personal data is:

- Processed only for the purposes for which they were collected.
- Not divulged to third parties without the subject's consent
- Relevant, accurate and up to date.
- Adequate but not excessive for the stated purpose.
- Disposed as confidential material when they are no longer needed for the purposes for which they were collected.

9. Staff responsibilities

- Staff members who process customer's personal data must comply with the requirements of this policy. Staff members must ensure that:
- All personal data is kept securely.
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party.
- Personal data is kept in accordance with the retention schedule.
- Any queries regarding data protection, including subject access requests and complaints, are promptly resolved.
- Any data protection breaches are swiftly brought to the attention of the Management.
- All passwords must be kept securely and changed regularly.
- All computers must be locked / logged off when away from desks.
- All confidential paper must be disposed securely by shredding.

- Employees must be complying with a 'clear desk' basis - by securely storing hard copy personal information when it is not being used.

Data & Documents Disposal Schedule

The time periods indicated are the maximum time period before destruction of the applicable information. PrePay may review and destroy earlier at its discretion if need for retention no longer exists.

Department & Data Description	**Retention Requirement**	**Classification**
Product/Account Management	**Retention Requirement**	**Classification**
Internal technical design docs	Permanent	Private
Jira/bug information	Permanent	Private
Processor documentation	3 Years	Private
Processor diagrams	1 Year After Most Current is Posted	Private
Product launch/go-to market materials	3 Years	Private
Product specifications	Permanent	Private
Vendor Contracts	7 years following termination of business relationship	Private

Risk	**Retention Requirement**	**Classification**
Beneficiary Information	Lifetime of Customer + 7 years	Private
Credit and Identity verification reports	Lifetime of Customer + 7 years	Private
Customer Accounts and Finance Reports	Lifetime of Customer + 7 years	Private

Customer Application	Lifetime of Customer + 7 years	Private
Customer correspondence	Lifetime of Customer + 7 years	Private
SAR Submissions & related correspondence	Lifetime of Customer + 7 years	Private

Customer Service	**Retention Requirement**	**Classification**
Complaints	Lifetime of Customer + 7 years	Private
Customer correspondence	Lifetime of Customer + 7 years	Private
Service interruption notices	5 Years	Private

Platform	**Retention Requirement**	**Classification**
Application logs, statistics, internal data	2 Years 3 Years	Private
Customer data and reports	Lifetime of Customer + 7 years	Restricted
Customer detailed data	Lifetime of Customer + 7 years	Restricted
Transactional data	7 years	Private
Application e-mail and notification records	3 Years 3 Years	Private

Marketing	**Retention Requirement**	**Classification**
Cookie and tracking data from web site Consents to storage of personal data	3 Years	Private
Inbound marketing data	3 Years	Private
Marketing collateral, campaign materials	3 Years	Private
Marketing emails	3 Years	Private

Marketing lists	3 Years	Private
Customer correspondence	3 Years	Private
Web site records/logs etc	3 Years	Private
Web site materials	3 Years	Private

Sales	**Retention Requirement**	**Classification**
Contact records in Salesforce Consents to storage of personal data	Permanent 3 years	Private
Inbound marketing data	2 years	Private
Marketing lists	3 years	Private
Customer correspondence	Lifetime of Customer + 7 years	Private
Site traffic records	3 years	Private

HR	**Retention Requirement**	**Classification**
CV	Permanent	Private
Consents to storage of personal data	Permanent	Private
Disciplinary records	Permanent	Private
Employment offers and contracts	Permanent	Private
Medical schemes	Permanent	Private
Pension and staff saving schemes	Permanent	Private
Performances reviews	Permanent	Private
Personnel records (terminated)	Permanent	Private
References		Private

Salary information	Permanent	Private
Sickness and health reports	Permanent	Private
Staff share & option schemes	Permanent	Private
Staff tests and investigation reports	Permanent	Private
Staff training materials	Permanent	Private
Time sheets	Permanent	Private
Training records	Permanent	Private
Wage records, salary, bonus payments, benefits, termination payments	Permanent	Private

Finance	**Retention Requirement**	**Classification**
Annual and quarterly financial statements	7 years	Private
Audit reports	Permanent	Private
Bank reconciliations	2 years	Private
Bank statements	3 years	Private
Business and strategic plans	5 years for formal plans	Private
Correspondence (general)	2 years	Private
Correspondence (legal and important matters)	Permanent	Private
Correspondence (with customers and vendors)	2 years	Private
Determination letter for income tax exemption	Permanent	Private
Depreciation schedules	Permanent	Private

Duplicate deposit slips	2 years	Private
Expense analyses/expense distribution schedules	7 years	Private
External audit investigations	Permanent	Private
Fraud and theft records	6 years minor, 10 years major	Private
Year-end financial statements	Permanent	Private
Insurance records, current accident reports, claims, policies, and so on (active and expired)	Permanent	Private
Internal audit reports	5 years	Private
Invoices (to customers, from vendors)	7 years	Private
Payroll records and summaries	7 years	Private
Purchase order records	7 years	Private
Retirement and pension records	Permanent	Private
Tax returns and worksheets	Permanent	Private
Trade licenses	Permanent	Private
Trademark registrations and copyrights	Permanent	Private

IT	**Retention Requirement**	**Classification**
3rd party licenses	Permanent	Private
Data breach reports and notices to authorities and impacted persons/entities	Permanent	Private

Equipment inventories and records, serial numbers etc.	While in use + 1 year	Private
PCI documentation	Permanent	Private
Security audits and penetration tests	3 years	Private

Governance	**Retention Requirement**	**Classification**
Board appointment documents	Permanent	Private
Board meeting papers	Permanent	Private
Board remuneration records	Permanent	Private
Company documentation, annual reports,	Permanent	Private
General correspondence/emails	3 years	Private
Minute books, articles and charter, certificates of incorporation/change of name	Permanent	Private
Investor documentation, reports and correspondence	Permanent	Restricted
Share certificates	Permanent	Restricted
Policy documents	Permanent	Private
Signatory mandates	Permanent	Private
Legal	**Retention Requirement**	**Classification**
Advices from counsel	7 years	Private
Authorizations and licenses	Life of license +2 years	Private

Contracts, mortgages, notes, and leases (expired)	7 years	Private
Contracts (still in effect)	Contract period + 3 years	Private
Court orders	Permanently	Restricted
Deeds, charges, mortgages, and bills of sale	Permanently	Restricted
General correspondence/emails	7 years	Private
Intellectual Property/Trademarks	Permanent	Private
Legal communications & correspondence	7 years	Private
Legal notices	3 years	Private
Legal research papers	7 years	Private
Litigation documents	7 years	Private
Practicing certificates	Until expiration	Private
Subpoenas	3 years or end of litigation	Private

R & D	**Retention Requirement**	**Classification**
Source code	Permanent	Private
Internal technical design docs	Permanent	Private