Data Protection Security Policy

VCPL-ISP-12 -V1.0

DOCUMENT AND RECORD CONTROL

Version Control

Document Control ID	VCPL-ISP-12 _Data Protection SecurityPolicy-V1.0
Issued Date	16-September-2022
Effective Date:	16-September-2022
Owner:	Infosec

Revision Table

Date	Version	Affected Sections	Author
16-September-2022	1.0		Mr Ramesh T.P

Release Authorization

Task	Author	Title
Prepared by	Mr Ramesh T.P	Deputy Vice President

Reviewer Authorization

Name	Title	Signature	Date
Mr. Prasenjit Datta	Head of Technology		16-September-2022

Approval Authorization

Name	Signature	Date
Board of Directors		

TABLE OF CONTENTS

1. Introduction

In its everyday business operations Vivriti Capital makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organization is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Vivriti Capital is taking to ensure that it complies with it. Vivriti Capital have adopted this Policy to govern the treatment of our customers' and employees' Personal Information. The loss of Personal Information can result in substantial harm to individuals, including embarrassment, inconvenience, and fraudulent use of the information. Protecting the confidentiality and integrity of Personal Information is a critical responsibility that must be taken seriously at all times. Compliance with this Policy is mandatory.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Vivriti Capital systems.

The following policies and procedures are relevant to this document:

- Data Protection Impact Assessment Process
- Personal Data Analysis Procedure
- Legitimate Interest Assessment Procedure
- Information Security Incident Response Procedure
- GDPR Roles and Responsibilities
- Records Retention and Protection Policy

2. Scope

The Policy applies to all Company employees, agents, and representatives, including any contractor or third-party provider of services to Vivriti Capital ("Third-Party Service Provider") who have access to Personal Information Vivriti Capital has collected or otherwise has in its possession. This Policy applies to all Personal Information collected, maintained, transmitted, stored, retained, or otherwise used by Vivriti Capital regardless of the media on which that information is stored and whether relating to employees, customers, or any other person.

3. Definitions

Personal Information

"Personal Information" means any information relating to an identified or identifiable natural or legal person (an "identifiable" person being one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity).

Privacy Laws

"Privacy Laws" means all applicable laws relating to privacy and the processing of Personal Information that may exist in any relevant jurisdiction.

Security Incident

"Security Incident" means an actual or reasonably suspected (a) unauthorized access to or acquisition, use, disclosure, alteration, or destruction of Personal Information; or (b) interference with a process, function or data on any Vivriti Capital or third-party information system that may adversely affect Vivriti Capital business operations.

4. Data Protection Policy

4.1 The General Data Protection Regulation

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that Vivriti Capital carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is Vivriti Capital's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

4.2 Definitions

There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

"**Personal data**" is defined as:

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.

"**Processing**" means:

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

"**Controller**" means:

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.

4.3 Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the GDPR is based.

These are as follows:

- Personal data shall be:
    - Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
    - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').
    - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization').
    - Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
    - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').
    - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').
- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Vivriti Capital will ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

4.4 Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Each of these rights are supported by appropriate procedures within Vivriti Capital that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown in Table 1.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling	Not specified

Table 1 – Timescales for Data Subject Requests

4.5 Lawfulness of Processing

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. It is Vivriti Capital policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described in brief in the following sections.

4.5.1 *Consent*

Unless it is necessary for a reason allowable in the GDPR, Vivriti Capital will always obtain explicit consent from a data subject to collect and process their data. In case of children below the age of 16 (a lower age may be allowable in specific EU member states) parental consent will be obtained. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject, then this information will be provided to the data subject within a reasonable period after the data are obtained and definitely within one month.

4.5.2 *Performance of a Contract*

Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g., a delivery cannot be made without an address to deliver to.

4.5.3 *Legal Obligation*

If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.

4.5.4 *Vital Interests of the Data Subject*

In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. Vivriti Capital will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. As an example, this may be used in aspects of social care, particularly in the public sector.

4.5.5 *Task Carried Out in the Public Interest*

Where Vivriti Capital needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

4.5.6 *Legitimate Interests*

If the processing of specific personal data is in the legitimate interests of Vivriti Capital and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

4.6 Privacy by Design

Vivriti Capital has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymization will be considered where applicable and appropriate.

4.7 Contracts Involving the Processing of Personal Data

Vivriti Capital will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR. For more information, see the GDPR Controller-Processor Agreement Policy.

4.8 International Transfers of Personal Data

Transfers of personal data outside the European Union will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

4.9 Data Protection Officer

Defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

4.10 Breach Notification

It is Vivriti Capital policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our Information Security Incident Response Procedure which sets out the overall process of handling information security incidents.

Under the GDPR the relevant DPA has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

4.11 Addressing Compliance to the GDPR

The following actions are undertaken to ensure that Vivriti Capital complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organization (if required)
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organization name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organizational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with data protection.

5. Using, Handling and Retaining Personal Information

5.1 Purpose

- As required applicable Privacy Laws, Vivriti Capital shall describe the purpose(s) for which Personal Information is collected, used, processed, disclosed, protected, and retained.
- Vivriti Capital shall collect, use, process, disclose, protect, and retain Personal Information in accordance with applicable Privacy Laws.
- Vivriti Capital shall collect, maintain, and use Personal Information that is accurate, complete, and relevant to the purposes for which it was collected.
- Personal Information collected must be limited to that which is reasonably necessary to accomplish Vivriti Capital legitimate business purposes or as necessary to comply with law.

5.2 Access, Use, and Sharing of Personal Information

- You may only access Personal Information when the information relates to and is necessary to perform your job duties. You may not access Personal Information for any reason unrelated to your job duties.
- You may not use Personal Information in a way that is incompatible with the purpose for which the information was collected. If you are unsure about whether a specific use or disclosure is appropriate, you should consult with the General Counsel.
- You may only share Personal Information with another Company employee, agent, or representative if the recipient has a job-related need to know the information. Personal Information may only be shared with a Third-Party Service Provider if it has a need to know the information for the purpose of providing the contracted services and if sharing the Personal Information complies with the applicable Privacy Laws which may require a fully executed written contract such as a Data Processing Agreement.

5.3 Data Subject Rights

Under certain Privacy Laws, individuals may have rights when it comes to how their Personal Information is handled. Individuals may exercise these rights by making a request to Vivriti Capital. These rights may vary depending on the applicable jurisdiction, but may include for example:

- **The right of access and/or portability**: A right to be provided with details of, and access to, the personal information Vivriti Capital processes about them (and if certain conditions apply, the ability to ‘port’ that personal information to another provider).
- **The right to rectification**: A right to obtain rectification without undue delay of inaccurate personal information Vivriti Capital processes about them.

- **The right to erasure**: A right for personal information about them to be erased from Vivriti Capital system on certain grounds.
- **The right to restriction**: A right to restrict Vivriti Capital processing of the individual's personal information on certain grounds.
- **The right to object**: A right to object, on grounds relating to his or her particular situation, to the processing of personal data about him or her, if certain grounds apply.
- **The right to object to sale of information**: A right to restrict Vivriti Capital from selling the individual's personal information.

This list is non-exhaustive, and individuals may be entitled to other rights not outlined above. You must comply with applicable Privacy Laws regarding the rights of Data Subjects. If you receive any requests from an individual exercising their rights, or if you are unsure about a request, please contact privacy@Vivriti Capital.com immediately. See our Individual Data Rights Procedure for more information.

5.4 Retention and Disposal

- You shall keep Personal Information only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. You must follow the applicable records retention schedules and policies and destroy any media containing Personal Information in accordance with the applicable records disposal policy.
- Any Personal Information no longer required to be retained under the applicable records retention schedule shall be disposed-off / destroyed / securely erased / anonymized regardless of the method of storage in a manner that prevents loss, theft, misuse, unauthorized access of Personal Information.

5.5 Security

- Vivriti Capital has implemented an Information Security Program (ISP) that sets forth technical, administrative and physical safeguards for the protection of Personal Information. The ISP includes appropriate monitoring and audit controls to support implementation of security controls to protect Personal Information.
- You must follow the security procedures set out in the ISP at all times and must exercise particular care in protecting Sensitive Personal Information from loss, unauthorized access of unauthorized disclosure.

6. Security Incident

If you know or suspect that a Security Incident has occurred, do not attempt to investigate the matter yourself. Immediately report it the Information Security Team according to the options set out below and follow the Security Incident Management Procedure.

Mechanism	Details	Description and Usage
Telephone		This is the most convenient and rapid way of reporting Security Incidents for customers. The number can be dialed for reporting Security Incidents and/or follow up.
Email		Reporting Security Incidents through email is also an efficient way. However, if the Security Incident is in the form of a network attack or targeted at the email system, the reporting channel may be affected. Alternative measures should be adopted to address such limitations, e.g., by using other reporting channels such as telephone.

You should preserve all evidence relating to the potential Security Incident. See our Security Incident Management Procedure for more information.

7. Training

All Vivriti Capital personnel who have access to Personal Information must be educated and trained on this Policy and the treatment of Personal Information. In addition, whenever Personal Information is entrusted to a Third-Party Service Provider, proper management and supervision over the outside party's handling of that Personal Information must be ensured through appropriate contracts. Personnel with responsibility for supervising employees or managing Third-Party Service Provider relationships must be trained on supervision over those employees and Third-Party Service Providers.

8. Monitoring Compliance and Enforcement

The General Counsel is responsible for administering and overseeing implementation of this Policy and, as applicable, developing related operating procedures, processes, policies, notices, and guidelines. If you are concerned that any provision of this Policy, or any related policy, operating procedure, process, or guideline designed to protect Personal Information, has been or is being violated, please contact the General Counsel directly or use _____ mail ID _____. The Company will conduct periodic reviews and audits to assess compliance with this Policy. Employees who violate this Policy and any related guidelines, operating procedures, or processes designed to protect Personal Information and implement this Policy may be subject to discipline.

---End of Document---