Omni-ISMS-DOC-A18-5
[Private]

# Privacy and Personal Data Protection Policy

Version 3
12TH FEBRUARY 2024

## Document Reference

| | |
|---|---|
| **Document:** | Omni-ISMS-DOC-A18-5 |
| **Document title:** | Privacy and Personal Data Protection Policy |
| **Filename:** | Omni-ISMS-DOC-A18-5 Privacy and Personal Data Protection Policy |
| **Author:** | Innovare |
| **Owner:** | Omni Strategies |
| **Date:** | 26th January 2022 |
| **Version:** | 3.0 |
| **Status:** | Final |
| **Retention:** | One (1) Year |
| **Archival:** | Two (2) Years |
| **Disposal:** | Three (3) Years |

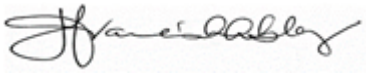
## Revision Record

| Version | Date | Summary of Changes | Revision Author |
|---|---|---|---|
| 1.0 | 26th January 2022 | Establishment of *Privacy and Personal Data Protection Policy* | Innovare |
| 2.0 | 20th January 2023 | No changes made | Omni Strategies |
| 3.0 | 12th February 2024 | No changes made | Omni Strategies |

## Distribution

| Name | Title |
|---|---|
| Executive Management | Omni Strategies |
| | |

## Approval

| Name | Position | Signature | Date |
|---|---|---|---|
| Dr Francis Blay | Chief Executive Officer |  | 20th February 2024 |

As a modern, forward-looking business, Omni Strategies recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.
In order to provide such a level of continuous operation, Omni Strategies has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001.

The operation of this ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

A Privacy and Personal Data Protection Policy is available in both paper and electronic form and will be communicated within the organization and to all relevant stakeholders and interested third parties.
Commitment to the delivery of information security extends to senior levels of the organization and will be demonstrated through the information security policy and the provision of appropriate resources to establish and develop the ISMS.
Top management will also ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that information security objectives are being met and relevant issues are identified through the audit programme and management processes.
A risk management approach and process will be used which is line with the requirements and recommendations of ISO/IEC 27001. Risk management will take place at several levels within the ISMS, including:

- Assessment of risks to the achievement of our information security objectives
- Regular information security risk assessments within specific operational areas
- Assessment of risk as part of the business change management process
- At the project level as part of the management of significant change

We would encourage all employees and other stakeholders in our business to ensure that they play their part in delivering our information security objectives.

Yours sincerely,
Francis Blay

## Table of contents

**1 INTRODUCTION ..... 5**

1.1 PURPOSE AND OBJECTIVES ..... 5
1.2 SCOPE ..... 6

**2 IMPORTANCE OF DATA PRIVACY ..... 7**

2.1 PHYSICAL SECURITY OF CUSTOMERS' DATA ..... 7
2.2 RECRUITING THE RIGHT STAFF ..... 7
2.3 TRAINING ..... 8
2.4 IT SYSTEMS ..... 8
2.5 IT RIGHTS ..... 8
2.6 RANDOM CHECKS ..... 8
2.7 DELETING DATA ..... 8

**3 DATA PROTECTION POLICY ..... 10**

3.1 STATUS OF THE POLICY ..... 10
3.2 NOTIFICATION OF DATA HELD AND PROCESSED ..... 11
3.3 RESPONSIBILITIES OF STAFF ..... 11
3.4 DATA SECURITY ..... 12
3.5 CUSTOMER OBLIGATIONS ..... 13
3.6 RIGHTS TO ACCESS INFORMATION ..... 13
3.7 SUBJECT CONSENT ..... 13
3.8 PROCESSING SENSITIVE INFORMATION ..... 14
3.9 THE DATA CONTROLLER ..... 14
3.10 BREACH NOTIFICATION ..... 14
3.11 DISCIPLINARY ACTIONS ..... 12

## List of Tables

## No table of figures entries found.

# 1 Introduction

The Data Protection Act, 2012 is one of the most significant pieces of legislation affecting the way that Omni Strategies carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the Data Protection Act, which is designed to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters. It is Omni Strategies policy to ensure that our compliance with the Data Protection Act and other relevant legislation is clear and demonstrable at all times.

In its everyday business operations Omni Strategies 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 following policies and procedures are relevant to this document:

- *Information Classification Procedure*
- *Information Labelling Procedure*
- *Acceptable Use policy*
- *Electronic Messaging Policy*
- *Internet Acceptable Use Policy*
- *ISMS Incident Response Procedure*
- *ISMS Roles, Responsibilities and Authorities*

## 1.1 Purpose and Objectives

This Privacy Policy describes how we collect, use, disclose, store and otherwise process information through our product and service platforms and through the products and/or services provided by or through other third-party partners supported by us as the back-end service provider. In addition, this privacy policy highlights how we control the collection, correction and/or deletion of information that personally belongs to customers. We will not use or share the information with anyone except as described in this Privacy Policy.

The purpose of this policy is to set out the relevant legislation and to describe the steps Omni Strategies is taking to ensure that it complies with it.

The objective of this policy is to ensure that Omni Strategies employees

- Are aware of their roles and responsibilities for data privacy of Omni Strategies clients.
- Safeguard client's personal data

## 1.2 Scope

This Data Privacy Policy applies to personal information and other information collected by Omni Strategies or its service providers using Omni Strategies platform in part or in full through or about:

a) Visitors to any Omni Strategies facilities, or users of, its products, websites;
b) Existing customers that are using the services pursuant to a written agreement with Omni Strategies written physically or virtually (online);
c) Prospective and or existing customers using the services pursuant to a browser wrap, or other online agreement;
d) Other service providers and partners of Omni Strategies;
e) Other third-parties that use any of Omni Strategies platform implemented on-site or Software-as-a-service (SaaS), including but not limited to the end users of prospective and existing customers.

Customer data is any identifiable personal information about a customer held in any format, such as national insurance numbers, address, date of birth, family circumstances, bank details and medical records.

# 2 Importance of Data Privacy

i. Customer data is a high value commodity for fraudsters and since service offerings of Omni Strategies require data from our customers in one form or another, securing it is also our responsibility.

## 2.1 Physical Security of Customers' Data

i. To ensure physical security of our customers' data, we implement strict security protocols over our customers' data, such as;

- Restricting access to the office by use of door finger print scanners
- Monitoring all visitors to our office by recording access, using signing in books with departure times and ensuring all visitors are supervised at all times
- Regular staff training
- Keeping files/filing cabinets locked and only accessible to appropriate staff
- Maintaining a clear desk policy
- Not sharing passwords and ensuring periodic compulsory change of passwords
- Ensuring computer servers are secured at all times

## 2.2 Recruiting the Right Staff

i. As a company, it is imperative that we have the right staff to work in our Company and whose responsibility it will be to manage data and implement security.

ii. When considering hiring staff, we operate a risk-based approach because, we believe by adopting this approach will help reduce the possibility of recruiting staff that may have been involved in perpetuating any form of financial crimes in the past, hence, we conduct extensive assessments and background checks including obtaining police clearance where necessary before staff into certain sensitive positions or departments in the company. This is imperative to ensure we recruit the best-fit at all times.

iii. Our risk-based approach ensures we continue;

- Recruiting appropriate staff with integrity, honesty, fit and proper for the role being recruited for
- Hold monthly appraisals /one-to-one's (which will help identify signs or any circumstances which could make staff more susceptible to financial crime)

## 2.3 Training

i. We are aware that many firms simply rely on staff signing an annual declaration to confirm they have read policies and procedures but do not check whether staff understands them.

ii. Omni Strategies always educates, guides and raises awareness on security through;

a) Group Discussions
b) Monthly security awareness sessions
c) Sending periodic awareness emails to all staff within the company
d) Rewarding examples of good practices within the company
e) Display of posters within the office to raise awareness

iii. These are simple, yet effective techniques to help our staff be vigilant and help company implement security.

## 2.4 IT Systems

i. Some of our staff may require access to customer data in order to perform their jobs and duties, but this is limited to our staff having only “relevant access”. By this we mean that staff will not be able to access information that they do not require to perform activities within the scope of their job functions.

## 2.5 IT Rights

i. When, and if, staff are required to change roles, their IT rights will be reviewed before they take on their new roles.

## 2.6 Random Checks

i. Designated management personnel of the company are tasked to conduct random and periodic checks on the backend to ensure that staff are accessing only relevant information and customer data.

## 2.7 Deleting Data

i. It is against company policy to delete customer data without written approval from the management.

a) Disabling USB ports/drives, CD Rom on computers if staff do not need them to perform their jobs
b) Clearing records/information in used laptops when being issued to new staff
c) Staff to change passwords every 90 days
d) Ensuring staff do not exchange passwords with colleagues
e) Ensuring staff do not write down passwords
f) Check which staff take office computers home

g) Have a system in place to manage stolen computers
h) Data encryption at all times

# 3 DATA PROTECTION POLICY STATEMENTS

i. Omni Strategies needs to keep certain information about its employees, customers and other users to allow it to monitor performance, achievements, and health and safety.

ii. For example, it is also necessary to process information so that staff can be recruited and paid, customer related transactions executed and legal obligations to report. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Omni Strategies must comply with the Data Protection Principles.

In summary these states that personal and customers data shall:

I. be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
II. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
III. be adequate, relevant and not excessive for those purposes.
IV. be accurate and kept up to date.
V. not be kept for longer than is necessary for that purpose.
VI. be processed in accordance with the data subject's rights.
VII. be kept safe from unauthorised access, accidental loss or destruction.
VIII. not be transferred to a country outside the area, unless that country has equivalent levels of protection for personal data.

iii. Omni Strategies and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Omni Strategies has developed the Data Protection Policy below:

## 3.1 Status of the Policy

i. This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Omni Strategies from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

ii. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the HR Department. If the matter is not resolved it should be raised as a formal grievance.

### 3.2 Notification of Data held and Processed

i. All staff and customers and other users are entitled to;

   i. know what information Omni Strategies holds and processes about them and why.
   ii. know how to gain access to it.
   iii. know how to keep it up to date.
   iv. know what Omni Strategies is doing to comply with its obligations

ii. Omni Strategies therefore provides all staff and customers and other relevant users with a standard form of notification. This will state all the types of data Omni Strategies holds and processes about them, and the reasons for which it is processed. Omni Strategies will ensure this is done at least once every three years.

### 3.3 Responsibilities of Staff

All staff are responsible for:

   i. checking that any information that they provide to Omni Strategies in connection with their employment is accurate and up to date.
   ii. informing Omni Strategies of any changes to information, which they have provided i.e., changes of address
   iii. checking the information that Omni Strategies will send out from time to time, giving details of information kept and processed about staff.
   iv. informing Omni Strategies of any errors or changes. Omni Strategies cannot be held responsible for any errors unless the staff member has informed Omni Strategies of them.

If and when, as part of their responsibilities, staff collect information about other people, (i.e., about customers course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are stated above.

All staff are required to complete training in Data Protection as component of their Induction to employment at Omni Strategies.

### 3.4 Data Security

i. All staff are responsible for ensuring that: Any personal data which they hold is kept securely. Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

ii. Staff are aware that unauthorised disclosure and/or failure to adhere to the requirements set out in "C to G" inclusive below will usually be a disciplinary matter, and may be considered gross misconduct in some scenarios.

iii. Personal and customer information should be; kept in a locked filing cabinet; or in a locked drawer; or if it is computerized, must be password protected; or when kept or in transit on portable media the files which must be password protected.

iv. Personal and customer data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites,

v. Ordinarily, personal and customer data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Data Controller in Omni Strategies must be obtained, and all the security guidelines given in this document must still be followed.

vi. Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:

- Suitable back-ups of the data exist
- Sensitive data is appropriately encrypted
- Sensitive data is not copied onto portable storage devices without first consulting a Data Controller, in regards to appropriate encryption and protection measures.
- Electronic devices such as laptops, mobile devices and computer media (USB devices etc.) that contain sensitive data are not left unattended when offsite.

vii. For some information the risks of failure to provide adequate security may be so high that it should NEVER be taken home. This might include payroll information, addresses of customers and staff, disciplinary or appraisal records or bank account details. Exceptions to this may only be with the explicit agreement of Executive Management.

### 3.5 Customer Obligations

i. Customers must ensure that all personal data provided to Omni Strategies is accurate and up to date. They must ensure that changes of address, etc. are notified to our office.

### 3.6 Rights to access Information

i. Staff, customers and other users of Omni Strategies products and services have the right to access any personal data that is being kept about them either on computer or in certain files.
ii. In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing, in the first instance to Omni Strategies IT Security/Data Protection Officer or through electronic means to be provided.
iii. Omni Strategies could possibly charge a fee on each occasion that access is requested, although Omni Strategies have discretion to waive this.
iv. Omni Strategies aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within the internal policy in place.

### 3.7 Subject Consent

i. In many cases, Omni Strategies can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to Omni Strategies to processing some specified classes of personal data is a condition of acceptance of a customer onto any service, and a condition of employment for staff. This may include information about previous criminal convictions.

ii. Omni Strategies may also ask its staff members for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes.

iii. Omni Strategies will only use the information in the protection of the health and safety of the staff member but will need consent to process in the event of a medical emergency, for example.

iv. All prospective staff and customers will be asked to sign a consent form to process data, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

### 3.8 Processing Sensitive Information

i. Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details.
ii. This may be to ensure Omni Strategies is a safe place for everyone, or to operate other policies of the company such as the sick pay policy or equal opportunities policy.
iii. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals. Staff will be asked to give express consent for Omni Strategies to do this.
iv. During a recruitment process, offers of employment may be withdrawn if an individual refuses to consent to this, without good reason.

### 3.9 The Data Controller

i. Omni Strategies as a Corporate entity is the ultimate data controller and the board is therefore ultimately responsible for implementation. However, there are designated data controllers who deal with day-to-day activities.
ii. The Company has designated one data controller, who is the primary point of authorisation for receipt and supply of data requests.

### 3.10 Breach Notification

i. In the event of breach of client's data, Omni Strategies shall contact the client's resource person in the next 48hrs. This will be managed in accordance with our *Incident Response Procedure* which sets out the overall process of handling information security incidents.

## 4 Disciplinary Statement

Non-compliance with this policy could have a significant effect on the efficient operation of Omni Strategies and may result in financial loss and an inability to provide necessary services to our customers. If any user is found to have breached this policy, they will be subject to disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

## 5 Exceptions

All waivers and exceptions to any portion of this policy statements must be duly approved by Omni's Chief Executive Officer.

## POLICY AMENDEMENTS AND REVISION

This policy can be changed modified, revised or rescinded completely by the company at any time with appropriate approvals.

***This document will be reviewed annually to ensure continual improvement of the ISMS; however, anytime there is a change in scope, regardless of the maintenance time, the document needs to be reviewed***