Data Protection and Privacy Policy

Document Control

The current version of this document is **Version 1.3,** approved 24 Mar 2023 by **Alison Swart**.

This document should be reviewed every **36 months** at a minimum.

Last Reviewed and Approved: Alison Swart 05 Sep 2022

Next Review Due Before: 24 Mar 2026

Purpose

The purpose of this document is to demonstrate Optimatics' commitment to the protection of Personal Data.

Policy

Optimatics operates primarily in the business of software development, licensing and support.

The Board, management and staff of Optimatics are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information and information-related assets to meet the purpose and goals of the organisation. This includes the handling of Personal Data or Personally Identifiable Information (PII).

Optimatics is committed to ensuring compliance with the European Union General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 1998, and any other data protection legislation or regulation relevant to our business operations. Optimatics will ensure staff and other relevant stakeholders and third parties are aware of their responsibilities when handling Personal Data.

More detailed policies and processes support this policy, including our Information Security Policy. These are located and managed within Confluence and the ISMS.online platform.

Scope

All employees of Optimatics and relevant interested parties (including directors, employees engaged through a related Suez entity, third party contractors, and volunteers) are required to comply with this policy.

Document Owner and Approval

Optimatics' CEO is the owner of this document and is responsible for ensuring that this policy document is reviewed regularly in line with the requirements set out in ISO 27001:2013.

Optimatics' Data Protection Officer (DPO) is responsible for the day-to-day implementation of this policy. They will monitor it regularly to ensure it is being adhered to.

This policy was approved by the ISMS Board and is issued on a version-controlled basis.

Definitions

The definitions of terms used within or referred to in the policy are based on those in the GDPR or other recognised documentation.

"**Consent**" of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of their Personal Data. [source GDPR]

"**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 processing of Personal Data. Where the purposes and means of such processing are determined by law, the Controller or the specific criteria for its nomination may be provided for by law. [source GDPR]

"**Customer Data**" includes, but is not limited to, any of these types of data:

- Personal Data
- Data provided by the customer for use by Optimatics in delivering support services
- Contractual information and terms

"**Data Subject**" means an identified or identifiable natural person 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person [source GDPR]

"**Personal Data**" and "**Personally Identifiable Information**" and "**PII**" means any information relating to a Data Subject

“**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. [source GDPR]

“**Processor**” means a natural or legal person, public authority, agency or other body, which processes Personal Data on behalf of the Controller. [source GDPR]

“**Processing**” means any operation or set of operations which is performed on Personal Data or 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. [source GDPR]

“**Profiling**” means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. [source GDPR]

“**Pseudonymisation**” means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person. [source GDPR]

“**Recipient**” means a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with any law shall not be regarded as Recipients. The Processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the Processing. [source GDPR]

“**Sensitive Personal Data**” is any information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings. Any use of Sensitive Personal Data must be strictly controlled in accordance with this policy. [source DPA]

1. Organisational Responsibilities

1.1 Specific Responsibilities

Chief Information Security Officer (CISO)	• Assumes full accountability for the information controlled and processed by the organisation including PII • Is the face and figurehead of Optimatics to interested parties. Holds a significant position in the business (C Level or one below), giving confidence to those parties that Optimatics takes data protection and information security seriously.
Data Protection Officer (DPO)	• Keeps the board updated about data protection responsibilities, risks and issues • Reviews all data protection procedures and policies on a regular basis • Arranges data protection training and advice for all staff members and those included in this policy • Answers questions on data protection from staff, board members and other stakeholders • Responds to individuals such as customers and employees who wish to know which of their data is being held by Optimatics • Checks and approves with third parties that handle the company’s data any contracts or agreements regarding data processing
Information Security Manager	• Ensures that information security risks have been identified and assessed, taking account of any special requirements for Personal Data. • Supports and advises other responsible managers and individuals in regards to information security requirements, policies & controls.
IT Manager	• Ensures all systems, services, software and equipment meet acceptable security standards • Checks and scans security hardware and software regularly to ensure it is functioning properly • Researches third-party services, such as cloud services, that Optimatics is considering using to store or process data
Marketing Manager	• Approves data protection statements attached to emails and other marketing copy • Addresses data protection queries from customers, target audiences or media outlets • Coordinates with the Data Protection Officer to ensure all marketing initiatives adhere to data protection laws and Optimatics’ Data Protection and Privacy Policy • Complies with other legislation and regulation relevant to data protection in marketing activities (eg. Privacy & Electronic Communications Act (UK))

1.2 Staff data protection training

All staff will receive training on this policy. New hires will receive training as part of the induction process. Ongoing training will be provided on a regular basis and when specific trigger events occur (eg. threats or incidents affecting all or part of the organisation, its supply chain or other interested parties that might impact the organisation financially or reputationally), or there is a substantial change in the law or Optimatics' policies and procedures. Completion of this training is compulsory and where appropriate will be evidenced by task completion in the ISMS.online platform.

Training will cover:

- The law relating to data protection
- Optimatics' data protection and related policies and procedures.

1.3 Transparency of data Processing

Optimatics commits to being transparent to individuals about how their Personal Data will be used, and to Processing data in accordance with the guidelines set out in this policy.

1.4 Conditions for Processing

Use of Personal Data is justified using at least one of the conditions for Processing (as set out below under *1.5.1 Fair and lawful Processing*). All employees who are responsible for Processing Personal Data will be aware of the conditions for Processing. The conditions for Processing will be available to Data Subjects in the form of this policy.

1.5 Justification for Personal Data

Personal Data will be processed in compliance with the data protection principles of the GDPR, and in accordance with this policy, as set out below.

Additional justification will be provided, and documented, for the Processing of Sensitive Personal Data. In most cases Processing of Sensitive Personal Ddata will require the Data Subject's *explicit* Consent, unless exceptional circumstances apply or it is required to be done by law (eg. To comply with legal obligations to ensure health and safety at work). Any such Consent will need to identify clearly what the relevant data is, why it is being processed and to whom it will be disclosed.

1.5.1 Fair and lawful Processing

Personal Data will be processed fairly and lawfully in accordance with individuals' rights. This will generally mean the individual whose details are being processed has Consented to this happening.

Under GDPR, Processing of Personal Data is lawful only if at least one of the following apply:

a) The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes;

b) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into the contract;

c) Processing is necessary for compliance with a legal obligation to which the Controller is subject;

d) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;

f) Processing is necessary for the purposes of the legitimate interests pursued by the Controller or a third party;

g) Except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

The Processing of all Personal Data must be:

- Necessary to deliver Optimatics' services.
- In the legitimate interests of Optimatics, and not unduly prejudice the individual's privacy.
- In most cases this provision will apply to routine business data processing activities.

1.5.2 Consent and revocation

The Personal Data collected by Optimatics is subject to active Consent by the Data Subject. This Consent can be revoked at any time.

1.5.3 Accuracy and relevance

Any Personal Data processed by Optimatics will be accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. Personal Data obtained for one purpose will not be processed for any unconnected purpose, unless the Data Subject has agreed to this or would otherwise reasonably expect this.

Individuals may ask that inaccurate Personal Data relating to them is corrected. If you believe that information is inaccurate, you should record the fact that the accuracy of the information is in dispute and inform the Data Protection Officer.

1.5.4 Data access and portability

Upon request, a Data Subject has the right to receive a copy of the data Optimatics holds on them in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals.

A Data Subject may also request that their data is transferred directly to another system. This must be done at no cost to the Data Subject.

Optimatics may, in the course of delivering its services, be required to give Personal Data to third parties, such as expert witnesses and other professional advisers.

1.5.5 Right to be forgotten

A Data Subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

1.5.6 Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Data Protection Officer will be responsible for conducting reviews of compliance with data protection laws, and ensuring that all IT and other relevant projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the Data Subject, privacy settings will be set to the most private by default.

1.5.7 International data transfers

Optimatics' will make it clear in the contract with each customer exactly where each type of Customer Data will be processed, and obtain the customer’s explicit Consent to their Customer Data being processed and stored in that geography.

1.5.8 Data security

Optimatics will keep Personal Data secure against loss or misuse. Where Personal Data is to be processed by a third party on behalf of Optimatics, the Data Protection Officer will establish what, if any, additional specific data security arrangements need to be implemented in contracts with that third party.

Optimatics has an “Information Security Policy” and a set of subordinate security policies and controls relating to the management of data and information security.

1.5.9 Data retention

Personal Data will not be retained for longer than is necessary. What is “necessary” will depend on the circumstances of each case, taking into account the reasons that the Personal Data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Data retention schedules will be maintained showing the minimum and maximum periods of retention for each data set.

2. Employee Responsibilities

All individual staff members are responsible for playing their part in maintaining the confidentiality, integrity and availability of Personal Data in compliance with the GDPR, DPA and organisational policies, standards and procedures.

Employees must be familiar with the requirements of this policy and any other relevant security policy, and comply with all requirements relating to the proper handling and security of Personal Data.

2.1 Employee Personal Data

Employees must take reasonable steps to ensure that Personal Data held about them is accurate and updated as required. Such things as a change of address, or other change in personal circumstances, should be advised to the Data Protection Officer or the Finance Team so the employee’s record can be updated.

2.2 Handling others’ Personal Data

Employees must comply with the requirements of this policy when handling Personal Data of others. Special care and attention must be given when handling Sensitive Personal Data.

2.3 Processing data in accordance with the individual's rights

Employees must comply with any request from an individual not to use their Personal Data for direct marketing purposes. Notify the Data Protection Officer about any such request if it falls outside of the normal processes, or you have any reason to be unsure about the appropriate practice.

Contact the Data Protection Officer for advice on direct marketing before starting any new direct marketing activity, to ensure compliance with all relevant data protection and other legislation.

2.4 Reporting breaches

All employees have an obligation to report to the Data Protection Officer actual or potential data protection weaknesses, events and incidents where compliance may be breached. This enables Optimatics to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

The reporting of such weaknesses, events and incidents will be managed through Optimatics' Information Security Incident Management processes.