Data Protection Policy

Last updated 1 Nov 2023

Version Control

Version #	Date	Updated by	Description
2.1	01/11/23	A Pope	Minor amendments
2.0	06/01/23	A Pope	Seamless Software adoption
1_9	01/01/21	R Baugh	Providing for Brexit and UK GDPR.
1_8	02/02/19	R Baugh	Clarifying GDPR v UK aspects, offences.
1_7	31/05/18	R Baugh	Removing reference to DPA 1998 Principles.
1_6	10/04/19	R Baugh	Reference to legal bases for processing.
1_5	09/04/18	R Baugh	Minor amendments.
1_4	06/04/18	R Baugh	Minor amendments.

DATA PROTECTION POLICY

Purpose

This Policy is a key part of Seamless Software's Data Protection Management System ('**DPMS**'). Its purpose is to ensure Seamless Software is compliant with its obligations under all applicable data protection laws ('**DP Laws**') and contracts or other interactions with stakeholders (including employees, customers, suppliers, partners, regulators and investors). The DPMS also aims to reduce or eliminate the potential for the commitment of, and liability for, criminal offences in DP Laws by Seamless Software and Seamless Software's officers and employees.

Scope

This policy applies to all Seamless Software officers and employees and, as appropriate, those operating on its behalf.

Please review the other policies within Seamless Software's DPMS which target particular risks and objectives such as the Encryption Policy and the Marketing & Personal Data Policy. In addition, security is fundamental to data protection and the DPMS closely interacts with Seamless Software's Information Security Management System ('**ISMS**') including related policies and procedures.

Interpretation

In this policy, we use definitions from the GDPR unless otherwise stated.

'**Anonymised data**' means information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

'**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.

'**DPIA**' means the PIA that must be carried out in certain situations, contain certain information, and over which there are other obligations, as set out in the GDPR.

'**EEA**' or '**European Economic Area**' means the EU and Iceland, Lichtenstein and Norway.

'**EU GDPR**' means the EU General Data Protection Regulation, 2016/679.

'**GDPR**' means either or both of the EU GDPR and UK GDPR. We will use this when there is little or no difference in the wording of the relevant law for the context.

'**Personal data**' means any information relating to an identified or identifiable natural person, namely one who can be identified, directly or indirectly from that information alone or in conjunction with other information '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'[1]. While '**personal data**' is a defined term in EU and UK law, we use it here to also cover '**personally identifiable information**' as defined in US law, and other similar legal definitions.

'**PIA**' means a privacy impact assessment, which is a written assessment of the risks to the rights and freedoms of data subjects through any processing of their personal data. A DPIA is just one type of PIA.

[1] Examples of personal data are from the EU GDPR.

'**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'.

'**Processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

'**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 (such as a lookup table relating alphanumeric identifiers to the individuals), 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.

'**Special Categories of Personal Data'** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

'Transfer' means the transfer of personal data either to '**third countries**' (meaning countries outside the EU for the EU GDPR or outside the UK for the UK GDPR) or '**international organisations**' (meaning an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries, such as the UN or WHO).

'**UK DPA**' means the UK Data Protection Act 2018.

'**UK GDPR**' means the UK-adopted version of the EU GDPR, which took effect from 1 January 2021 as a result of Brexit.

The Policy

Seamless Software is committed to ensuring that any processing of personal data by or on behalf of Seamless Software is carried out in compliance with DP Laws. Data relating to legal entities is also protected in a small number of countries and, where Seamless Software collects or processes such data from such countries, we will treat it as personal data within our DPMS.

Seamless Software will comply with the GDPR including its six core principles ('**6 Principles**') set out in Article 5 of the GDPR, which in summary are:

1. Lawfulness, fairness and transparency
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. Purpose limitation
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Data minimisation
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy

Personal data shall be 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.

5. Storage limitation
Personal data shall be 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.

6. Integrity and confidentiality
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, when Seamless Software as controller, processes personal data, one of the 6 legal bases set out in Article 6 of the GDPR must apply to ensure lawful processing:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. the 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 a contract;
3. the processing is necessary for compliance with a legal obligation to which the controller is subject;
4. the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. the 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;
6. the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, 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 (this basis is not available to support processing carried out by public authorities in the performance of their tasks).

Where Seamless Software wishes to process Special Categories of Personal Data, or personal data relating to criminal convictions and offences or related security measures, we must comply with additional requirements. Please see the Sensitive Personal Data Policy.

Seamless Software **as 'controller' and 'processor'**

While, in all cases, processing of personal data must be in accordance with applicable DP Laws:

- where Seamless Software is the controller, we will comply with all obligations applicable to controllers in DP Laws. Seamless Software as with most businesses, is the controller of the majority of personal data we process, for example across employee relations, marketing and finance activities, and supplier management.

- where Seamless Software is the processor, the relevant personal data may only be processed in accordance with the contract we have with, and the instructions of, the controller. Seamless Software will also comply with any obligation on processors in DP Laws.

Risk-based Approach

The DPMS mirrors the GDPR and is a risk-management based system and any and all measures taken under the DPMS are to be appropriate to the risk in question. This means that, in some instances, lesser measures are required (for example in the protection of purely

public Information) while in other instances significant measures are required (for example in the protection of Special Categories of Personal Data).

Governance

As part of its DPMS, Seamless Software has committed to maintain a governance structure to ensure compliance with DP Laws, including the following.

Senior Sponsorship

The Compliance Officer has overall responsibility for establishing and maintaining the DPMS. Responsibility for the creation and maintenance (including appropriate periodic review) of this document, and related policies and procedures, shall be clearly set out in each such document.

Responsibilities

While senior sponsorship is set out above, we all have responsibilities to ensure we appropriately process and protect personal data in accordance with DP Laws and the DPMS, including (as appropriate to our roles) reporting personal data breaches, carrying out PIAs, carrying out due diligence on processors, and otherwise implementing privacy by design and privacy by default across Seamless Software's business. Staff must ensure they are fully aware of the DPMS as it relates to their roles as they are responsible for compliance by Senior Leadership and by suppliers for whom they are the lead.

Policies & Procedures

Seamless Software will establish and maintain appropriate policies to ensure compliance with applicable DP Laws across the data lifecycle, and appropriate procedures to ensure that the policies may be put into practice. Policies will address governance and risk across the personal data lifecycle from collection to destruction.

Training & Awareness

Seamless Software will train staff on the importance of data protection and aspects of this DPMS as appropriate to their role and level of seniority at on-boarding, on change of role and with refresher training sessions as appropriate.

Records

Seamless Software will establish and maintain records required to demonstrate compliance, such as the privacy notices provided to data subjects, records of consent, and Article 30 Records.

Security Measures

As a fundamental requirement under GDPR, Seamless Software will maintain appropriate technical and organizational measures against unauthorized or unlawful processing of personal data held or controlled by Seamless Software and against accidental loss or destruction of, or damage to, such personal data. The security measures will address the need to maintain the required confidentiality, integrity and availability of personal data, including the use of encryption according to our Encryption Policy and appropriate back-up practices.

Review

As appropriate, Seamless Software will review developments in DP Laws and codes of practice and practical changes in working patterns, assess the DPMS against any such development, and consider any required update to the DPMS.

Consent

Whenever consent is to be the legal basis for processing personal data, such consent must be obtained in accordance with the requirements of DP Laws and Consent Procedure, recorded appropriately and an appropriate mechanism for withdrawal provided.

Collection, Transparency & Purpose Limitation

Addressing the GDPR's 1st Principle (Lawfulness, fairness and transparency) and 2nd Principle (purpose limitation), Seamless Software shall provide the information required (in particular under Articles 13 and 14 of the GDPR) in a privacy notice to data subjects at the appropriate time in order for processing of that personal data to be lawful, fair and transparent. The privacy notice will be delivered in a compliant manner for the particular context, whether by single notices, layered notices, tooltips and other suitable methods. Seamless Software shall ensure that the purposes are included in the information provided to data subjects and respected during processing.

Privacy by Design & Privacy by Default

Seamless Software shall adopt policies and procedures to implement privacy by design and privacy by default into its working practices as appropriate. Key areas include the design and use of technology, storage, security systems including access to data, and marketing. We will carry out PIAs and DPIAs as appropriate and in accordance with our PIA & DPIA Policy. We will also consider the use of anonymisation and pseudonymisation as appropriate and will use encryption as set out in our Encryption Policy.

HR

Seamless Software shall ensure that all processing of personal data concerning officers and employees is processed according to our HR Privacy Notice at all times. Background checks must not be carried out without consulting HR and criminal reference checks must not be carried out without consulting Legal and in accordance with our Sensitive Personal Data Policy.

Data Subject Rights

Data subjects – individuals about whom we process personal data - have several rights under the GDPR and other DP Laws. Seamless Software shall always respect data subjects' rights and their exercise of them in accordance with those laws and shall respond to the exercise of such rights in accordance with our Data Subject Rights Policy and related procedures.

Sensitive Data

Given its business, Seamless Software processes the gender of individuals under the age of 18, and this falls under Special Categories of Personal Data in our DIPA. Seamless Software does not process data relating to criminal conviction and offences other than for its own human resources purposes. These types of personal data are given much higher protection under DP Laws and as such are referenced in our DIPA and Data Processing Agreement

Children's Data

Seamless Software processes personal data related to individuals under the age of 18.

- Name
- School year group
- Gender

Financial Data

Seamless Software will comply with the PCI Data Security Standard ('**PCI DSS**') at all times when processing credit card data. The PCI DSS provides an actionable framework for

developing a robust payment card data security process, including prevention, detection and appropriate reaction to security incidents.

Anonymisation

Where appropriate, Seamless Software shall anonymise personal data that is not held within the secure school login. As anonymised data is not personal data, the DP Laws do not apply to any processing of anonymised data. As a result, anonymisation should be considered throughout the data lifecycle although it may not be practical in many circumstances other than the end of a retention period, where personal data may be anonymised as opposed to securely deleted or destroyed under our Information Deletion & Destruction Policy. Any anonymisation carried out by or on behalf of Seamless Software must satisfy legal and regulatory requirements as well as any Anonymisation Procedure we have adopted at that time.

Pseudonymisation

Unlike anonymised data, pseudonymised data is still personal data as individuals can be re-identified by use of additional information, such as a lookup table linking individuals to alphanumeric identifiers. Seamless Software shall therefore protect, retain, delete and otherwise process pseudonymised data in the same way as other personal data.

However, pseudonymisation is an excellent tool to reduce risk in certain circumstances and is likely to be applicable on many more occasions throughout the data lifecycle than anonymisation. Seamless Software shall consider pseudonymisation when appropriate and any pseudonymisation carried out by or on behalf of Seamless Software must satisfy legal and regulatory requirements as well as any Pseudonymisation Procedure we have adopted at that time.

Marketing

All marketing activities must comply with our Privacy & Marketing Policy, its related procedure, and all applicable laws at all times.

Use of processors

The choice and use of processors or sub-processors shall be in accordance with our Processor (Vendor) Policy.

Transfers

Transfers of personal data to third countries or international organisations shall only be carried out in accordance with our Transfers Policy.

Retention & End-of-Life

In accordance with our Retention Policy, Seamless Software shall first honour its legal obligations as to the period for which any particular personal data must be kept. Subject to any such legal obligation, we shall consider any exercise by a data subject of their rights in light of all relevant factors under DP Laws. At the end of the retention period for particular personal data, that personal data shall either be anonymized or securely deleted or destroyed under our Information Deletion & Destruction Policy.

Criminal offences

As well as the potential maximum fines in the EU / UK GDPRs of €20m / £17.5m or 4% of global turnover, whichever is higher, national laws typically set out criminal offences for certain processing of personal data contrary to that nation's DP Laws. Such offences typically include obtaining or sharing personal data unlawfully, causing personal data to be altered

without authorisation, and re-identifying individuals without authorisation. Seamless Software will always have a lawful basis or lawful authorisation for its processing of personal data.

Approved Codes of Conduct & Certifications

The GDPR allows for approval of codes of conduct (Article 40) and certification mechanisms (Article 42). Adherence to an approved code or certification mechanism may be used as an element by which to demonstrate compliance with various requirements in the GDPR. If necessary or appropriate, Seamless Software will review such codes and certification mechanisms for relevance and fit for our operations.

Breach

If you become aware of a breach of this policy, you must report it promptly to the Compliance Officer andrew.pope@seamlesssoftware.co.uk

Enforcement

All Seamless Software employees bear responsibility for their own compliance with this policy. Breach of this policy is ground for disciplinary proceedings against an employee, which may result in disciplinary action including termination of employment. Breach of this policy by any non-employee such as a temporary worker, contractor or supplier may be a breach of their contract with Seamless Software and grounds for damages or termination.

Ownership

The Compliance Officer is responsible for maintaining this policy and related training and awareness programs.