DATA PROTECTION POLICY

Contents

Document Management

Version	Name	Revision Date	Change
2.0	Peter Johnston (Citation)	07/08/2024	Rewrite following upgrade to ISO 27001:2022

Responsibility and Authority

The Smarterpay Executive holds overall authority.

Responsibility	Appointment
Periodic review and maintenance	ISO Committee
Release approval	CTO

Objectives

To ensure that the use of personal information is controlled in accordance with the Data Protection Act 2018 and General Data Protection Regulations principles and that an individual's rights are respected.

Document Scope

This Policy applies to all Information Assets, including those relating to Company, customer and development information across the Company and where personal data is processed by external providers.

Responsibilities

Data Protection Officer: Responsible for reviewing the details of potential or actual breaches of personal data notifications to ensure that these are referred to the ICO. Additional requirements for notification may also arise from Personal Data Impact Assessments. The Data Protection Officer has direct responsibility for DP procedures, including Subject Access Requests.

IT Staff: To ensure that data protection controls are implemented, and records maintained.

Employees and Contractors: For ensuring that data protection controls are followed and for notifying the Data Protection Officer of concerns or breaches of personally identifiable information (PII). All staff employed by the Company are also responsible for ensuring that any personal data that is about them that they supply is accurate and up to date.

Management: Shall ensure their employees and contractors comply with this Policy.

Data Protection Introduction

The Company needs to collect and use certain types of information about staff and other individuals who come into contact with it to operate. In addition, it may be required by law to collect and use certain types of information to comply with the statutory obligations of Local Authorities, government agencies and other bodies.

This personal information must be dealt with properly. However, it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this is within the EU General Data Protection Regulation and the Data Protection Act.

The Data Protection Officer retains a record of notifications to the ICO. The ICO Notification Handbook is used as authoritative guidance for notifications. This record is reviewed annually, and update notifications are issued accordingly.

Any breach of the GDPR will be considered a breach of the Disciplinary Policy and could also be considered a criminal offence, potentially resulting in prosecution.

Third parties working with or for the Company and who have or may have access to personal information will be expected to comply with this Policy. Before access is permitted, third parties who require access to personal data will be required to sign a Confidentiality Agreement. This agreement will also include an agreement that the Company can audit compliance with the Confidentiality Agreement.

The Company is a data controller and/or a data processor as defined under GDPR and the Data Protection Act 2018.

Data Protection Principles

Any processing of personal data must be conducted in accordance with the following data protection principles of the Regulation, and Company policies and procedures will ensure compliance.

Personal data must be processed lawfully, fairly and transparently.

The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' 'rights and freedoms'.

Information must be communicated to the data subject in an intelligible form using clear and plain language.

Management is responsible for ensuring that all staff are trained in the importance of collecting and maintaining accurate data.

All individuals are responsible for ensuring that any data held by the Company is accurate and up to date. Any data submitted by an individual to a Company, such as via a registration form, will be considered to be accurate at the time of receipt.

Employees or other individuals should notify the Company of any changes in personal information to ensure it is kept up to date. It is the company's responsibility to ensure that any notification of changes to personal information is implemented.

The Data Protection Officer is responsible for ensuring that all necessary actions are taken to ensure that personal information is accurate and up to date. This should also consider the volume of data collected, the speed with which it might change and any other relevant factors.

The Data Protection Officer will review, at least once a year, all the personal data processed by the Company held in the Data Register. The Data Protection Officer will note any data that is no longer required in the context of the registered purpose and will ensure that it is appropriately removed and securely disposed of.

If a third party has provided inaccurate or out-of-date personal information, the Data Protection Officer is responsible for informing them that the personal information is inaccurate and/or out-of-date and will advise them that the information should no longer be used. The Data Protection Officer should also ensure that any correction to the personal information is passed on to the third party.

Personal Data

Personal data must be kept in a form that allows the data subject to be identified only as long as necessary for processing.

Where personal data is retained beyond the processing date, it will be encrypted to protect the data subject's identity in the event of a data breach.

Personal data will be retained in line with the retention of records procedure, and once its retention date is passed, it must be securely destroyed.

Personal data must be processed in a manner that ensures its security.

Appropriate technical and Company measures shall be taken against the unauthorised or unlawful processing of personal data and against the accidental loss or destruction of, or damage to, personal data. These controls have been selected based on identified risks to personal data and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to audit and review.

Compliance with this principle is contained in the Information Security Management System (ISMS), which has been developed in line with ISO 27001:2022 and the Security Policy set out in the ISMS.

Personal data shall not be transferred to a country or territory outside the European Union Member States unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the EU Member States is prohibited unless one or more of the specified safeguards or exceptions apply.

An assessment of the adequacy is carried out by the data controller, considering the following factors:

- The nature of the information being transferred
- The country or territory of the origin and final destination of the information
- How the information will be used, and for how long
- The laws and practices of the country of the transferee, including relevant codes of practice and International obligations and
- The security measures that are to be taken as regards the data in the overseas location.

Accountability

The GDPR states that the controller is responsible for ensuring compliance and demonstrating that each processing operation complies with the GDPR's requirements. As a result, controllers are required to keep all necessary documentation of all processing operations and implement appropriate security measures. They are also responsible for completing Data Processing Impact Assessments (DPIAs), complying with requirements for prior notifications or approval from supervisory authorities and ensuring a Data Protection Officer is appointed if required.

Data Subjects' Rights

Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of the automated decision-taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by an automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data
- To request the ICO to assess whether any provision of the GDPR has been contravened

- The right for personal data to be provided to them in a structured, commonly used and machine-readable format and the right to have that data transmitted to another controller
- The right to object to any automated profiling without consent
- Data subjects may make data access requests. The Data Protection Officer reviews these and processes them so that the procedure ensures that the response complies with the regulations' requirements.

Complaints

A Data Subject has the right to complain at any time to the Company if they have concerns about how their information is used. If they wish to lodge a complaint, this should be directed to the Data Protection Officer.

A Data Subject also has the option to complain directly to the Information Commissioner's Office. Details of the options for lodging a complaint should be provided.

Consent

'Consent' is taken by the Company to mean that agreement to the processing of personal data has been explicitly and freely given and that this consent is specific, informed and an unambiguous indication of the data subject's wishes. The consent of the data subject can be withdrawn at any time.

The Company also takes consent on the basis that it has been given by the data subject, who is fully informed of the intended processing and is in a fit state of mind and without undue pressure to give consent being applied.

There must be some active communication between the parties, which demonstrates active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Consent to process personal and sensitive data is obtained routinely using standard consent documents. This may be through a Contract of Employment or during initial induction.

Data Security

Company staff that are responsible for any personal data must keep it securely and ensure that it is not disclosed under any conditions to any third party unless that third party has been specifically authorised to receive that information and has entered into a confidentiality agreement.

Personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Aspects Policy. You should form a judgment based on the sensitivity and value of the information in question, but personal data must be kept:

- In a lockable room with controlled access and/or
- In a locked drawer or filing cabinet and/or
- If computerised, it must be password protected in line with the Password Policy
- Stored on encrypted removable media.

PC screens and terminals must be hidden from view except by authorised staff. Staff must review the Acceptable Use Policy before they are given access to Company information.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit (written) authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

Manual records that have reached their retention date are to be shredded and disposed of as 'Confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed. Because of the increased risk, all staff must be specifically authorised to process data off-site.

Data Access Rights

Data subjects have the right to access any personal data (i.e. data about them) held in electronic format and manual records that form part of a relevant filing system. This includes the right to inspect confidential personal references and information obtained from third parties about that person.

Disclosure of Data

The Company ensures that personal data is not disclosed to unauthorised third parties, including family members, friends, government bodies and, in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not a disclosure of the information is relevant to and necessary for the conduct of business operations.

GDPR permits a number of exemptions where certain disclosure without consent is permitted as long as the information is requested for one or more of the following purposes:

- To safeguard National Security
- Prevention or detection of crime, including the apprehension or prosecution of offenders
- Assessment or collection of tax duty
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)
- To prevent serious harm to a third party
- To protect the vital interests of the individual - this refers to life and death situations.

Requests to provide data for one of these reasons must be supported by appropriate paperwork, and the Data Protection Officer must specifically authorise all such disclosures.

Data Retention, Deletion and Disposal

Personal data may not be retained for longer than it is required. Some data will be kept for longer periods than others. Data is deleted in accordance with the defined Record Retention Period for each record type held by the Company.

Personal data must be deleted and/or disposed of in a way that protects the 'rights and freedoms' of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion, or obfuscation of personally identifiable data).

Principles for deletion of records held on cloud services are identical to non-cloud records.

GDPR Risk Assessment

The Company needs to ensure that it is aware of any risks associated with processing all types of personal information. To assess any risk to individuals during the processing of their personal information, the company has implemented a risk assessment procedure.

Assessments will also be completed for any processing undertaken on their behalf by any third-party organisation. By applying the Risk Assessment procedure, the Company ensures that any identified risks are managed appropriately to reduce the risk of non-compliance.

Where the processing of personal information may result in a high risk to the 'rights and freedoms' of natural persons, the Company will complete a data protection impact assessment prior to conducting the processing to ensure the personal information is protected. This assessment may also be used to apply to a number of similar processing scenarios with a similar level of risk.

Where, as a result of a Data Protection Impact Assessment, it is clear that the Company will process personal information in a manner that may cause damage and/or distress to the data subjects, the Data Protection Officer must review the process before the Company proceeds to process the information. If the Protection Officer decides that there are significant risks to the data subject, they will escalate to the ICO for final guidance. The Company will apply selected controls for the ISO 27001 Annex A to reduce risk. This also references the Company's risk acceptance criteria and the requirements of the GDPR and The Data Protection Act 2018.