Square Daisy

Data Protection Policy

V1.0 - Approved

24th May 2018

Contents

Document Control

Document History

- Version 1.0
- Date - 24th May 2018
- Status - Approved
- Description - New Policy

Document Approval and Ownership

- Owner - Jovan Marić
- Title - Managing Director and DPO
- Approval Date - 24th may 2018
- Date of Review - 23rd May 2019

_____

Signature

1. Introduction

Square Daisy is committed to complying with the law and regulations in (all) our business(es) and activities, including applicable Data Protection Laws.

This policy, and the associated policies, set out the expected behaviours of Square Daisy's employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data held within the business.

2. Scope

Personal Data is any information (including opinions and intentions) which relates to an identified or 'Identifiable Natural Person'. Personal Data is subject to certain legal safeguards and other regulations which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. Square Daisy, as Data Controller is responsible for ensuring compliance with the data protection requirements outlined in this framework and the associated documents.

The Information Commissioner's Office (ICO) is responsible for upholding information rights in the public interest and enforcing the requirements of UK Data Protection Laws.

The specific objective of this policy and associated policies is to ensure that all employees understand the requirements to comply with Data Protection Laws in relation to data held on customers, employees, contractors and other named individuals, for example, those working for our business partners.

This policy applies to all processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy does not contain an exhaustive set of requirements. Employees should remember to comply with the spirit of the policy. The policy is subject to continuous review and new pages and/ or amendments may be issued from time to time. It is the responsibility of the individual to ensure they have access to the current version at all times.

If an employee or any associated person does not understand how the policy applies to them, or what action they should take they should speak to their manager.

The scope of this policy will apply to all companies owned by Square Daisy where a Data Subject's Personal Data is processed:

- In the context of our business activities
- For the provision or offer of services to individuals (including those provided or offered free of charge) by our business
- To actively monitor the behaviour of individuals (including using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to analysing or predicting their personal preferences, behaviours and attitudes.

Furthermore, the policy applies to all employees, contractors or third parties who may handle data on behalf of Square Daisy. Square Daisy will ensure that all Third Parties engaged to Process Personal Data on their behalf are aware of and comply with this policy.

3. Definitions

Personal Data	Any information (including opinions and intentions) which relates to an identified or identifiable natural person.
Identifiable natural person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as name, and identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controller	A 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.
Data Subject	The identified or identifiable natural person to which the data refers.
Process, processed, processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include 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.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Protection Authority	An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulations – in the UK this is the ICO.
Data Processors	A natural or legal Person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
Third Country	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Profiling	Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an identifiable natural person. In particular to analyse or predict certain aspects concerning that natural person's performance at work economic situations, health, personal preferences, interests, reliability behaviour, location or movement.
Personal Data Breach	A breach of security leading to the accidental or unlawful; destruction, loss, alteration, unauthorised disclosure of, of access to, Personal Data transmitted, stored or otherwise Processed.
Encryption	The process of converting information or data into code, to prevent unauthorised access.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a key that allows the data to be re-identified.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.
GDPR	The General Data Protection Regulation

4. Roles and Responsibilities

All employees, including contractors and third parties who process data on behalf of Square Daisy are responsible for complying with the requirements of this policy.

The DPO is responsible for maintaining the policy, maintaining an up to date and accurate ICO Registration, ensuring compliance with any Data Subject requests and ensuring incidents are reviewed and managed accordingly.

All Department Heads are responsible for ensuring that documented procedures are in place to comply with the requirements of this policy.

5. Policy

5.1. Data Protection Principles

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means Square Daisy must tell the Data Subject what Processing will occur (transparency), the Processing must match the description give to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation(lawfulness).

Principle 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. This means Square Daisy must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 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. This means Square Daisy must not store any Personal Data beyond what is strictly required.

Principle 4: Accuracy

Personal Data shall be accurate and kept up to date. This means Square Daisy must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 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 is Processed. This means Square Daisy must, wherever possible, store Personal Data in a way that limits or prevents identification of Data Subjects.

Principle 6: Integrity & 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. Square Daisy must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means Square Daisy must be able to demonstrate that the six Data Protection Principles outlines above are met for all Personal Data for which it is responsible.

5.2. Data Collection and Processing

Data Source

Personal Data should only be collected from the Data Subject if one of the following conditions apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject MUST be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation.
- A national law expressly provides for the collection, processing or transfer of the Personal Data.

Where notification is required, it should given promptly and in any case no later than:

- One calendar month from the first collection or recording of the Personal Data.
- At the time of first communication if used for communication with the Data Subject.
- At the time of disclosure if disclosed to another recipient.

5.3. Data Subject Consent

Square Daisy will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their Personal Data Square Daisy is committed to seeking such consent.

5.4. Data Subject Notification/External Privacy Notices

Square Daisy will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the processing of their personal data.

When a Data Subject is asked to give consent to the processing of personal data and when any personal data is collected from the Data Subject, all appropriate

disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or consent

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in approved by the business. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

Each external website owned by Square Daisy will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

5.5.Data Use

Data Processing

Square Daisy uses the Personal Data of its customers for the following broad purposes:

- Personal details are inputted to the financial software, Xero, for accounting purposes. These details include name, business e-mail, business address, business telephone and other company details that the individual is linked to, but this is the limit of personal details
- We hold business e-mail addresses for some clients which act as a username or retrieval e-mail for their website access. These are held along with a password which are stored in 1Password which is GDPR compliant
- We hold name, business e-mail, business address, business telephone and other company details that the individual is linked to on our e-mail accounts storing correspondence from clients between us (the team) and them
- E-mail addresses and some business contact details are passed between the team using Slack to enable communications between various members of the team and our clients
- Some individual business details are added to Asana which is our project management system to enable communications between various members of the team and our clients on specific projects or elements of projects
- Personal details from individuals are held on the individual LinkedIn accounts of our team for communications and messaging through that channel
- We have name, business e-mail, business address, business telephone and other company details that the individual is linked to on our mobile phones where applicable for contacting customers
- We hold personal details of customers relating to their businesses in Harvest for time tracking - these details are not accessed through Harvest itself but

integrate with Xero and Asana where some personal details are kept for invoicing and project management purposes

- Customer and prospect data is held within our CRM system called Mautic. This enables us to reach out to clients with marketing information and updates. All this data has been gathered with consent and not purchased from third party organisations and always carries an option to unsubscribe or opt out of future correspondence. All future enquiries and customer data will be subject to 'opt-in' requests

The use of the customer's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Square Daisy will process personal data in accordance with all applicable laws and applicable contractual obligations. Square Daisy will not process personal data unless one of the following conditions are met:

- The Data Subject has given consent to the processing of their personal data for one or more specific purposes
- 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
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person
- 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 Data Controller
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller of by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child)

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. These cases should be referred to the DPO for further advice.

5.6.Special Categories of Data

Personal Data will only process special categories of data (also known as sensitive data) where the Data Subject expressly consents to such processing or where one of the following conditions apply:

- The Processing relates to personal data which has already been made public by the Data Subject

- The Processing is necessary for the establishment, exercise or defence of legal claims
- The Processing is specifically authorised as required by law
- The processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health

Personal Data will only Process special categories of data with the explicit consent of the Data Subject.

5.7. Data Quality

Square Daisy employees will ensure that the personal data they collect and process is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject by:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification
- Following the Retention and Deletion Policy

5.9.Digital Marketing

Square Daisy will not send promotional or direct marketing material to customers through digital channels such as mobile phones, email and the internet without first obtaining their consent. The Data Subject must be informed that they have the right to object to direct marketing at any stage. If the Data Subject puts forward an objection, digital marketing related processing of their personal data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision.

It should be noted that where digital marketing is carried out in a 'business to business' context there is no legal requirement to obtain an indication of consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

5.10.Data Retention

To ensure fair processing, personal data will not be retained by Square Daisy for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. In order to comply with our regulatory obligations we will store personal data for a period of 7 years after purpose for which it was originally collected has been completed. During this storage period no further processing of personal data will be carried out unless the customer requests it or a complaint is made. Further details are set out in the Data Retention and Deletion Policy.

5.11.Data Protection

Square Daisy will adopt physical, technical and organisational measures to ensure that security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access of processing, and other risks to which it may be exposed by virtue of human action of the physical or natural environment.

Data security and protection measures are set out in the Square Daisy Information Security Policy.

5.12.Data Subject Requests

Square Daisy has established procedures to enable and facilitate the exercise of Data Subject Rights relating to:

- Information access
- Objection to Processing
- Restriction of Processing
- Data portability
- Data rectification
- Data erasure

If a Data Subject makes a request relating to any of the rights listed above Square Daisy will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing, and upon successful verification of their identity, the following information about their own personal data:

- The purpose of the collection, processing, use and storage of their personal data
- The source(s) of the personal data, if it was not obtained from the Data Subject
- The categories of personal data stored for the Data Subject
- The recipients or categories if recipients to whom the personal data has been or may be transmitted, along with the location of those recipients
- The envisaged period of storage for the personal data or the rationale for determining the storage period
- The use of any automated decision-making, including profiling

The right of the Data Subject to:

- Object to processing of their personal data
- Lodge a complaint with the Data Protection Authority
- Request rectification or erasure of their personal data
- Request restriction of processing of their personal data

A response to any request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification checks will be carried out to confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects have the right to require Square Daisy to correct or supplement erroneous, misleading, outdated or incomplete personal data.

If Square Daisy are unable to fully respond to the request within 30 days, Square Daisy will provide the following information to the Data Subject or their authorised legal representative within the specified time:

- An acknowledgment of receipt of the request
- Any information located to date
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision
- An estimated date by which any remaining responses will be provided
- An estimate of any costs to be paid by the Data Subject (where the request is excessive in nature)
- The name and contact information of the DPO

If responding to a request would disclose personal data about another individual, the information must be redacted or withheld as may be necessary or appropriate to protect the rights of the other individual.

Detailed guidance for dealing with requests from Data Subjects can be found in the Square Daisy Data Subject Request Handling Procedures document.

5.13.Law Enforcement Requests & Disclosures

In certain circumstances Square Daisy will be required share Personal Data without the knowledge or consent of a Data Subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the Order of a court or by any rule of law

If Square Daisy Processes personal data for one of these purposes then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If any employee receives a request from a Court or any regulatory or law enforcement authority for information relating to a Square Daisy customer this must be immediately brought to the attention of the DPO.

5.14.Data Transfers

Square Daisy may need to transfer data internally or to third parties in order to meet business requirements. Square Daisy will only transfer data to third party recipients outside the EEA where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects and/or where the appropriate security measures are in place.

Square Daisy may only transfer personal data where one of the transfer scenarios listed below applies:

- The Data Subject has given consent to the proposed transfer
- The transfer is necessary for the performance of a contract with the Data Subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of a Data Subject
- The transfer is legally required on important public interest grounds
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the vital interest if the Data Subjects

5.15. Transfers to Third Parties

Square Daisy will only transfer Personal Data to, or allow access by, third parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where third party processing takes place Square Daisy will first identity if, under applicable law, the third party is considered a Data Controller or a Data Processor of the personal data being transferred.

Where the Third Party is deemed to be a Data Controller Square Daisy will enter into an appropriate agreement with the controller to clarify each party's responsibilities in respect to the personal data transferred. Where the third party is deemed to be a Data Processor Square Daisy will enter into an adequate processing agreement with the Data Processor. The agreement must require the Data Processor to protect the personal data from further disclosure and to only process personal data in compliance with Square Daisy instructions. In addition the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification of personal data breaches.

When Square Daisy is outsourcing services to a third party (including cloud computing services), they will identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any third country transfers of personal data. In either case it will make sure to include adequate

provisions in the outsourcing agreement for such processing and third country transfers, this will include the provision for regular audits.

5.16.Complaint Handling

Data Subjects with a complaint about the processing of their personal data should direct their complaint for the attention of the DPO. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The DPO will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the Data Subject and the DPO, then the Data Subject may at their option, seek redress through mediation, binding arbitration, litigation or via complaint ICO.

5.17.Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the DPO using the usual breach notification procedures.

5.18.Data Protection By Design and Default

Article 25 of the GDPR states:

" (1)....the controller shall, both at the time of the determination of the means of processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as Pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

A Data Protection Impact Assessment (DPIA) must be conducted for all new and/or revised systems or processes.

6. Training

All employees will have their responsibilities under this policy outlined to them as part of their induction training. All employees will complete an annual refresher of this training. Square Daisy will provide further training and guidance if there are any updates made to this policy and/or the associated policies and procedures.

7. Monitoring Compliance

As a minimum the following will be monitored to ensure compliance with this policy:-

- An annual Data Protection Compliance Audit which will, at the minimum assess:
    - Compliance with policy in relation to the protection of personal data, including;
        - The assignment of responsibilities.
        - Raising awareness.
        - Training of employees.
    - The effectiveness of Data Protection related operational practices, including;
        - Data subjects rights.
        - Personal Data transfers.
        - Personal Data incident management.
        - Personal Data complaints handling.
    - The level of understanding of Data Protection policies and privacy notices.
    - The currency of Data Protection policies and privacy notices.
    - The accuracy of Personal Data being stored.
    - The conformity of Data Processor activities.
    - The adequacy of procedures for redressing poor compliance and Personal Data Breaches.

The Square Daisy and key business stakeholders will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by Square Daisy.

8. Review

This policy is owned by Jovan Marić and will be reviewed at least annually. We will provide information and/or training on any changes we make.

9. Related Documents

- Retention and Deletion Policy
- Data Breach Notification Procedure
- Privacy and Internet Cookies Notice
- Information Security Policy