Papermule Ltd

GDPR Data Protection Policy

CONTENTS

Table of Contents

Document History

Date	Author	Change
2018-12-10	Mike Hoy	Original
2019-01-29	Mike Hoy	Re-Written to separate out Employee and Public Privacy policy content

1. Introduction

Papermule Ltd is committed to protecting the rights and privacy of individuals and will process personal data in a fair and lawful manner.
The General Data Protection Regulation (Regulation 2016/679) ("GDPR") is one of the most significant pieces of legislation affecting the way that Papermule carries out its information processing activities. It is Papermule's policy to ensure that our compliance with the GDPR and applicable national legislation is clear and demonstrable at all times.

Who is responsible for this policy?

The Directors of Papermule have overall responsibility for the day-to-day implementation of this policy. You can contact any of the Papermule Directors for further information about this policy.

Related Policies
This Data Protection Policy should be read in conjunction with these other Papermule policies;

- Employee Privacy Policy
- Public Privacy Statement
- Internet Technology Security Policy

1.1. Data Protection Officer

The Directors of Papermule Ltd have examined the criteria mandating the appointment of a Data Protection Officer and also that of the requirement to register with the Information Commissioners Office.
We recognise that we are not a public authority or body, we don't monitor individuals or process any special categories of personal data or data relating to criminal convictions and offenses. Given that, and the technical nature of the services provided by Papermule and the high ratio of Directors to staff, we consider the appointment of a Data Protection Officer a potential hindrance in being able to respond quickly and effectively. We have therefore taken the position that the provision of the Data Protection Officers responsibilities be borne instead by the company Directors.

1.2. Information Commissioners Office

The Directors of Papermule Ltd have examined the requirements placed upon a business to register with the Information Commissioners Office.
Following guidance on the Information Commissioners Office web site and whist recognising that Papermule is only a data controller for the purposes of payroll, employment and business activities, Papermule Ltd is not legally required to register with the Information Commissioners Office.

2. Scope and Purpose

2.1. Scope

This policy applies to the processing of personal data in relation to identified or identifiable natural persons from any source and is part of Papermule's approach to compliance with data protection law.

In our everyday business operations Papermule makes use of a variety of data about identifiable individuals, including but not limited to data about:

- current, past and prospective employees;
- current, past and prospective customers;
- users of our website;
- other stakeholders (including but not limited to suppliers and contractors).

All Papermule staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal.

2.2. Purpose

The purpose of this Data Protection Policy is to enable Papermule to:

- Ensure compliance with applicable UK and EU law;
- Ensure that Papermule does everything possible to respect the rights and privacy of all data subjects whose data Papermule may hold or use;
- Protect Papermule, our staff, customers and other individuals from the consequences of a data breach;

3. Definitions and Terminology

Appendix 1 sets out the most fundamental definitions in the context of this policy.

4. The Principles

Papermule Ltd policies and procedures are designed to ensure compliance with the principles upon which GDPR is based. All processing of personal data must be conducted in accordance with these principles.

The Principles are:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

The lawful basis for which Papermule can process personal data is outlined in Section 8.

2. Limited for its purpose

Data can only be collected for specific, explicit and legitimate purposes.

Personal data collected and stored by Papermule will only be used for the purposes it was collected for. Processing of existing data for new purposes will require the completion of a DPIA as outlined in Section 14.

3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

Papermule will ensure that only the data required to identify the individual and provide the benefit or service requested is collected and stored. This data will not be duplicated unnecessarily.

4. Accurate

The data we hold must be accurate and kept up to date.

Papermule promote accurate data collection and entry and where possible validate this through process checks. Data storage is also centralised in searchable repositories to reduce data duplication and enable ease of data maintenance.

5. Retention

We cannot store data longer than necessary.

Papermule has in place procedures for the regular review of stored personal data and an archive and destruction process to ensure it is only kept for legitimate legal reasons.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

Papermule stores personal data (in hard or digital media) in secure storage which has appropriate security measures in place to provide suitable levels of access to those needing to process it. Digital data is protected from accidental loss, destruction or damage through secure digital backup strategies.

5.Accountability and transparency

Papermule shall be responsible for, and be able to demonstrate compliance with the six principles outlined above.
Papermule will ensure that adequate records in the following areas are maintained:

- The processing of personal data
- IT Systems Security Audits
- Policy Reviews

6.Lawful basis for processing data

All personal data must be processed in a lawful manner and it is Papermule's policy to identify under which of the following six basis that that processing will take place. Ensure that any data you are responsible for processing has a written lawful basis approved by a Papermule Director.

At least one of the following conditions must apply whenever we process personal data:

1. Consent

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose. Consent of the data subject means 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 (e.g. Opt-in as opposed to Opt-out), signifies agreement to the processing of personal data relating to him or her. Consent may be obtained by a number of methods including but not limited to:

- Clauses in customer contracts;

- Check boxes on replies forms;
- Online forms with check boxes where personal data is collected;

2. *Contract*

The processing of data necessary to fulfil or prepare a contract for the individual does not require explicit consent of the individual. e.g. the delivery of an order cannot be made without an address to deliver to.

3. *Legal obligation*

We have a legal obligation to process the data (excluding a contract) in order to comply with the law. Explicit consent is not required from the individual. Papermule's legal obligations around employment and taxation would be relevant examples.

4. *Vital interests*

Processing the data is necessary to protect a person's life or in a medical situation.

5. *Public function*

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. *Legitimate interest*

The processing is necessary for Papermule's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

7. Special categories of personal data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

Where Papermule processes special categories of personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

The processing of special categories of data will require a Papermule Directors prior approval.

8.Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. Papermule must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from a Papermule Director.

4. Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.

- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

9.Subject Access Requests

What is a subject access request?

An individual has the right to request and receive confirmation that their data is being processed, access to their personal data and supplementary information.
Papermule's Public Privacy Statement provides details of the data that may be collected, stored, processed along with details to make such a request.

How we deal with subject access requests

We must provide an individual with a copy of the information they request, free of charge. This must occur without delay, and within one month of receipt of a valid request. A valid request will likely necessitate requisite proof of identification. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.
If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from a Papermule Director before extending the deadline.
We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from a Papermule Director.
Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from a Papermule Director first.

10. Papermule's Data Protection Responsibilities

10.1. Processes and Procedures

Papermule's approach to implementing and maintaining GDPR compliance is based on the introduction of processes and procedures to ensure necessary steps are taken and recorded when introducing new data handling procedures. Coupled with this is the parallel introduction of an on-going review process to ensure these procedures and processes are maintained and fulfilling the desired purpose.

A significant aspect of the introduction of a new data handling procedure includes the completion of a Data Protection Impact Assessment (DPIA). Papermule's DPIA sets out to question and document the following:

- Identify the need
- Describe the processing
    - Nature
    - Scope
    - Context
    - Purpose
- Consultation
- Assess Necessity / Legality / Proportionality
- Identify and Asses Risk
- Identify Measurers to reduce risk
- Record Outcomes

A Papermule DPIA Template has been created to assist in this process and contains more descriptive requirements.

10.2. Contractual

Papermule

Papermule as a Data Controller and Processor deals with a variety of personal data pertinent to the day to day business operation of the business. The data managed includes that of past, current and future employees, contractors, customers and suppliers and is legitimised through consent, contract and legal obligation.

Papermule as Service Provider

Papermule provides a variety of services to prospective, current and past customers. Before undertaking any data processing activities Papermule will ensure that a relevant written contract or equivalent are in place.
Contracts will clearly set out the responsibilities of the respective parties and clearly communicate the instructions of the Data Controller to Papermule, the Data Processor. All contracts will specify:

- The purpose of transfer and processing
- The Type and Categories of Data
- Term and Termination
- Security measures

- Processing Restrictions
- Data Retention / Destruction

10.3. Sub-Processing

From time to time Papermule uses the services of sub-contractors and suppliers for the provision of support and or services.
Prior to a sub-contractor or supplier being provided any access to personal data Papermule will ensure a DPIA has taken place and a written contract entered into with that party.
Contractual terms will include:

- The Purpose of data transfer and permitted processing activities
- Security requirements
- Term and Termination
- Processing Restrictions
- Data Retention / Destruction
- Right to Audit

10.4. Transferring data internationally

GDPR restricts the transfers of personal data outside the EEA ("European Economic Area") and any transfers will require individually reviewing by a Papermule Director. The outcome of such a review would implement process, procedures and or contractual obligations in the form of Model Contract, SCC's and or Binding Corporate Rules.

10.5. Maintaining Records

DPIA Records

Papermule will ensure that all Data Protection Impact Assessments result in a record being added to the relevant register.
Records will contain the following information:

- Who undertook the Assessment
- When the Assessment took place
- Who or What the Assessment was for

Processing Records

Papermule will maintain a record of processing activities that take place within the business involving personal data. Records will contain the following information:

- Organisation name and relevant details
- Purposes of the personal data processing
- Categories of individuals and the personal data processed
- Categories of personal data recipients
- Agreements, mechanisms and controls in place.
- Relevant technical and organisational controls in place.

Training Records

Papermule will maintain a record of all training and CPD session provided in relation to GDPR whether formal or otherwise.
Records will contain the following information:

- Who provided the training / information?
- Who received the training / information?
- When it took place
- What was covered
- Remedial action(s) to be taken.

10.6. Personal Data Breach and Notification

A personal data breach is 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 by Papermule. This includes both paper and digital formats.

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach.
All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the appropriate parties

Papermule Ltd also has a legal obligation to report data breaches where there is the likelihood and severity of a risk to people's rights and freedoms to the information commissioner's office within 72 hours.

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.
Please report any potential or actual occurrences by email to the Papermule Directors (directors@papermule.co.uk)

11. Training

All Papermule staff will undergo GDPR Awareness Training and CPD sessions covering various relevant aspects of GDPR pertinent to their current role.
If you require additional training on data protection matters, contact one of the Papermule Directors.

12. Appendix A - Definitions

Data controller	means Papermule and anyone else who (either alone or jointly with others) determines the purposes and means of the processing of personal data;
Data processor	means anyone who processes data on behalf of an organisation for the purposes set out in this policy.
Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. *Business purposes include the following*: • Compliance with our legal, regulatory and corporate governance obligations and good practice • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Provision of technical support for products or services offered by Papermule • Ensuring business policies are adhered to (such as policies covering email and internet use) • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking • Investigating complaints • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments • Monitoring staff conduct, disciplinary matters • Marketing our business • Improving services
Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*

Special categories of personal data	As defined in Section 7
Processing	'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.