DATA PROTECTION POLICY

1. Introduction

Origins of CJM needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the business's data protection standards and to comply with the law. This policy applies to all personal data processed by Origins of CJM.

2. Why this policy exists

This data protection policy ensures Origins of CJM:

complies with data protection legislation including the General Data Protection Regulation (GDPR) and follows good practice (follows the eight data protection principles set out in Schedule 1 to the Act) and

- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data and
  Protects itself from the risks of a data breach

3. Definitions

The following definitions are used in this policy:

Controller	means the person or organisation that determines when, why and how to process Personal Data. We are the Data Controller of all Personal Data used in our organisation for our own purposes
Data Subject	means a living, identified or identifiable individual about whom we hold Personal Data
Data Privacy Impact Assessment (DPIA)	means a tools and assessment used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of Personal Data.
Personal Data	means any information identifying a Data Subject or information relating to a Data Subject form which we can identify (directly or indirectly) a Data Subject whether from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special category Personal Data and Pseudonymised Personal Data

	but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data Breach	means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach
Privacy Notice	means a notice setting out information that should be provided to Data Subjects when we collect information about them
Processing or Process	means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. processing also includes transmitting or transferring Personal Data to third parties
Special Category Personal Data	means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and relating to criminal offences and convictions

4. Data Protection Principles

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The law requires that Personal Data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
  Be accurate and kept up-to-date
- Not be held for any longer than necessary, in any event for a minimum of 6 years, except in the case of Subscribers to our marketing materials.
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

We are required to enable Data Subjects to exercise certain rights in relation to their Personal Data.

We must also comply with particular legal requirements when suppliers that carry out services for us have access to Personal Data and when we are working with organisations and need to share Personal Data.

We are responsible for and must be able to demonstrate compliance with the requirements under the law (accountability).

5. Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The law restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The lawful bases available when processing non-special category personal data are:

- the Data Subject has given consent to the processing of his or her personal data for one or more specific purposes

- the processing is necessary for the performance of a contract between us and the Data Subject or in order to take steps at the request of the Data Subject prior. to entering into a contract.

- the processing is necessary for compliance with a legal obligation to which we are subject.

- the processing is necessary in order to protect the vital interests of the Data. Subject or of another natural person
- the processing is necessary for the performance of a task carried out in the public interest

- the processing is necessary for the purposes of legitimate interests we are pursuing or which a third party is pursuing, 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.

A range of additional legal requirements apply when processing **special category personal data**. One of the lawful basis identified above is required as well as a separate lawful basis from the following list:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection providing for appropriate safeguards for the fundamental rights and the interests of the data subject

- 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

- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

- processing relates to personal data which are manifestly made public by the data subject

- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

- processing is necessary for reasons of substantial public interest

- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

- processing **is necessary for reasons of public interest** in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

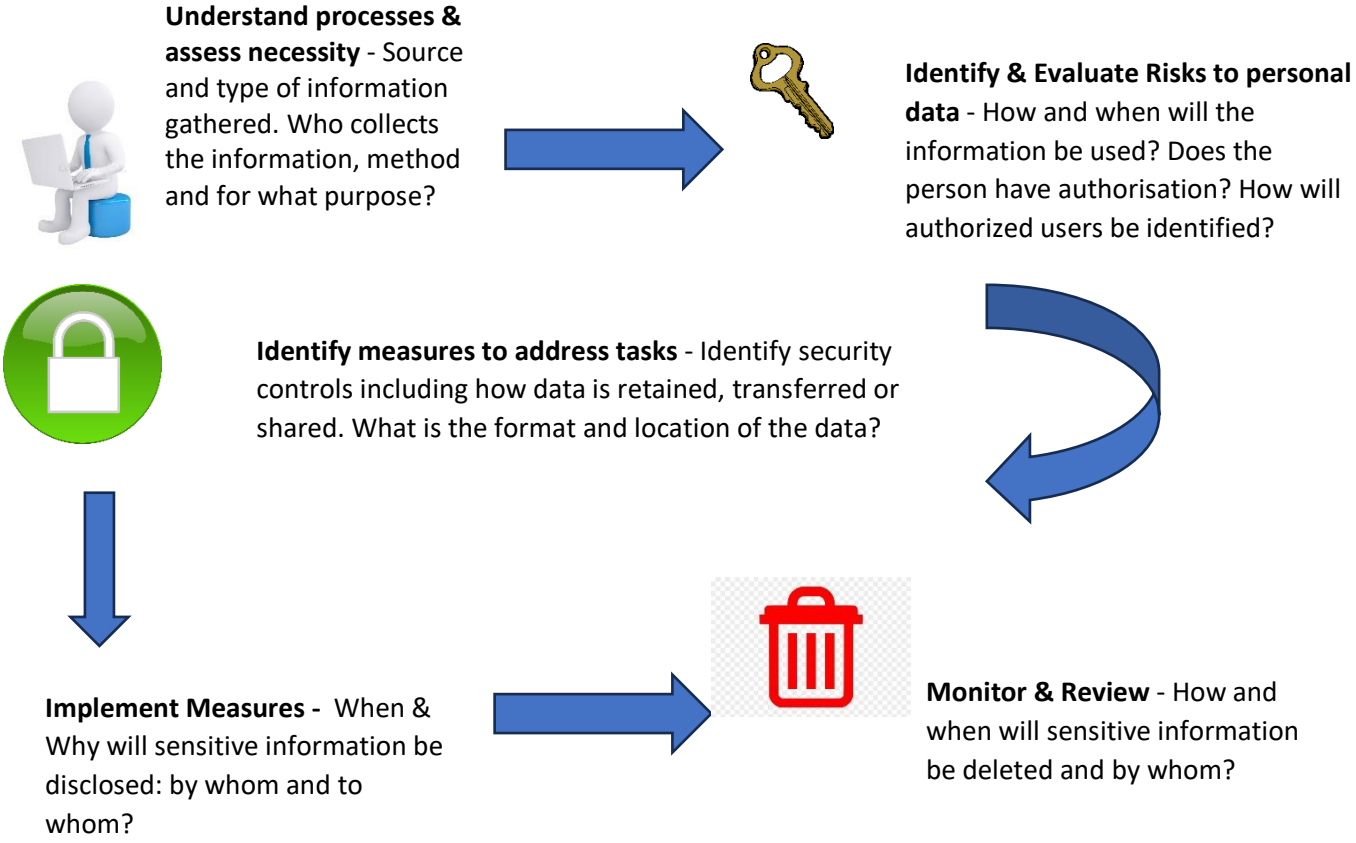
6. Transparency

The law requires us to provide detailed, specific information about our use of Personal Data to Data Subjects. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, we must provide the Data Subject with information including who we are and how and why we will Process, disclose, protect, and retain their Personal Data. This is done through a **Privacy Notice** which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with the Privacy Notice information as soon as possible but no later than one month after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with law and on a lawful basis which contemplates our proposed Processing of that Personal Data.

Where appropriate a DPIA assessment will be carried using the process highlighted in the diagram below:



7. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. You cannot use Personal Data for new, different, or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and there is a lawful basis for doing so.

This policy applies to Origins of CJM. It applies to all data that the business holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

– Names of individuals
– Postal addresses
– Email addresses
– Telephone numbers
– Plus, any other information relating to individuals

8. Data protection risks

This policy helps to protect Origins of CJM from some very real data security risks, including:

Breaches of confidentiality. For instance, information being given out inappropriately.

Failing to offer choice. For instance, all individuals should be free to choose how the business uses data relating to them.

Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

9. How does Origins of CJM keep your information safe

Origins of CJM makes every effort to keep your information safe and secure and has measures in place to ensure that your information, regardless of whether it is held on a computer or in paper files. Examples of our security measures include:

- Everyone who works for or with Origins of CJM has some responsibility for ensuring data is collected, stored, and handled appropriately.
- When the business handles personal data, it must ensure that it is handled and processed in line with this policy and data protection principles.
- The business owner is ultimately responsible for ensuring that Origins of CJM meets its legal obligations. The business owner is also the Data Protection Manager.
- General staff guidance on managing data.
- Secure storage arrangements to protect records and equipment to prevent loss, damage, theft, or compromise of personal information.
- Strong user access and password controls that help to ensure that only authorised individuals have access to Origins of CJM information and systems.

The Data Protection Manager who in this case is also the business owner is responsible for:

Keeping updated about data protection responsibilities, risks, and issues.

Reviewing all data protection procedures and related policies, in line with an agreed schedule.

Arranging data protection training and advice for the people covered by this policy.

Handling data protection questions from staff and anyone else covered by this policy.

Dealing with requests from individuals to see the data Origins of CJM holds about them (also called 'subject access requests').

Checking and approving any contracts or agreements with third parties that may handle the business's sensitive data.

Ensuring all systems, services, and equipment used for storing data meet acceptable security standards.

Performing regular checks and scans to ensure security hardware and software are functioning properly.

Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

Approving any data protection statements attached to communications such as emails and letters.

Addressing any data protection queries from journalists or media outlets like newspapers.

Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

10. General staff guidelines

The only people able to access data covered by this policy should be those who need it for their work.
Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

Origins of CJM will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

In particular, strong passwords must be used, and they should never be shared.

Personal data should not be disclosed to unauthorized people, either within the company or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees should request help from their line manager or the data protection manager if they are unsure about any aspect of data protection.

11. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the business owner or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

When not required, the paper or files should be kept in a locked drawer or filing cabinet.

Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

Data should be protected with strong passwords that are changed regularly and never shared between employees.

If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.

Data should be backed up frequently.

All servers and computers containing data should be protected by approved security software.

12. Data use

Personal data is of no value to Origins of CJM unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

Personal data should never be transferred outside of the European Economic Area.

Employees should not save copies of personal data on their personal computers. Always access and update the central copy of any data.

13. Data accuracy

The law requires Origins of CJM to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Origins of CJM should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

14. Subject access requests

All individuals who are the subject of personal data held by Origins of CJM are entitled to:

Ask what information the company holds about them and why.

Ask how to gain access to it.
Be informed about how to keep it up to date.
Be informed about how the company is meeting its data protection obligations.

If an individual contacts the business requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at originsofcjm@gmail.com.

Individuals will not be charged per subject access request. The data controller will aim to provide the relevant data within 30 calendar days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

The following Data Subject Rights will apply:

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data.

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection.

Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if Origins of CJM was processing the data using consent or on the basis of a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless Origins of CJM can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claim.

15. Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, originsofcjm@gmail.com will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the business's legal advisers where necessary.

16. Retention

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. We will maintain retention policies and procedures to ensure Personal Data is deleted in accordance with this requirement.

17.Providing information

Origins of CJM aims to ensure that individuals are aware that their data is being processed and that they understand:

How the data is being used
How to exercise their rights

To these ends, the business has a privacy statement, setting out how data relating to individuals is used by the business which is available on the website.

Date of Review July 2023