**Privacy and Document Retention Policy**

**Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Date | Summary of Changes | Initial |
| A | Mar 21 | Revised policy created by Birketts | **ED** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Privacy & Document Retention Policy**

**Contents**

1. INTRODUCTION

2. POLICY SCOPE

3. GENERAL STAFF GUIDELINES

4. DATA RETENTION

5. DATA USE

6. DATA ACCURACY

7. SUBJECT ACCESS REQUESTS

8. DISCLOSING DATA FOR OTHER REASONS

9. PROVIDING INFORMATION

# Introduction

Hethel Innovation Ltd. 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 company’s data protection standards — and to comply with the law.

## Why this policy exists

This data protection policy ensures Hethel Innovation Ltd:

* Complies with data protection law and follows good practice
* Protects the rights of staff, customers and partners
* Is open about how it stores and processes individuals’ data
* Protects itself from the risks of a data breach

## Data protection law

The Data Protection Act 1998 and the General Data Protection Regulation (GDPR) describes how organisations – including Hethel Innovation Ltd – must collect, handle and store personal information.

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 Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful basis
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

The General Data Protection Regulation adds to these:

1. Specific legal basis for collecting and processing personal data
2. The right of the individual to access, correct, or delete personal data

# People, risks and responsibilities

## Policy scope

This policy applies to:

* All staff of Hethel Innovation ltd
* All Directors operating within their role at Hethel Innovation Ltd
* All contractors, suppliers and other people working on behalf of Hethel Innovation Ltd.

It applies to all data that Hethel Innovation holds relating to identifiable:

* Private Individuals - People who have provided Hethel Innovation Ltd with personal data without a connection to an established limited business or who operate a business as a soletrader or partnership
* Individuals representing businesses - People who have provided Hethel Innovation Ltd with personal data in connection to their role within an established limited business

This can include:

* Names of individuals
* Postal addresses
* Email addresses
* Telephone numbers
* plus any other information relating to an individual

## Legal Basis

Hethel Innovation Ltd works with a range of data sources from different individuals and organisations requiring different legal basis for collecting and processing personal data.

### Contractual obligation

Our contractual relationships with other organisations and individuals (e.g. ERDF partners, or client businesses) mean that we collect and process their personal data.

We have a lawful basis for collecting and processing personal data where there is a standing contract which requires personal data from an individual to comply with the obligations of the contract.

### Legitimate Interest

Hethel Innovation Ltd provides a range of services as both a business service provider and as a business wholly owned by Norfolk County Council. Our primary interest in all activities undertaken by Hethel Innovation is the increased resilience of our local economy through the creation / growth of businesses and the creation of jobs.

For these purposes, we process personal data (e-mail addresses, names, phone numbers) to keep businesses and third parties informed of opportunities and progress. Any and all communications created by Hethel Innovation Ltd comply with e-privacy rules on consent.

### Affirmative Consent

Where we must collect and process personal information from a private individual Hethel Innovation seeks affirmative consent from that person. This is done in two clear ways: through our websites, users are given the details of how their data will be used and are asked to consent to that information being used; in physical forms we ask that the person consent to the collection and processing of their data through our signed forms.

## Data protection risks

This policy helps to protect Hethel Innovation Ltd 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 Hethel Innovation uses data relating to them.
* Reputational damage. For instance, the project could suffer if hackers successfully gained access to sensitive data.

## Responsibilities

Everyone who works for or with Hethel Innovation Ltd has responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

If any employee recognises an error in how we collect, store, or process data it is their responsibility to inform the Data Protection Officer.

However, these people have key areas of responsibility:

* The **Managing Director** is ultimately responsible for ensuring that Hethel Innovation Ltd meets its legal obligations.
* The **Data Protection Officer** is responsible for:
	+ Keeping the board 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 access, update, or delete the data Hethel Innovation Ltd holds about them.
	+ Checking and approving any contracts or agreements with third parties that may handle the project’s sensitive data.
	+ 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

# 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.
* **Hethel Innovation Ltd 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 unauthorised 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 officer if they are unsure about any aspect of data protection.

# Data Retention

## The retention of data

Hethel Innovation Ltd stores data both physically and digitally and as such has policies in place to ensure that this data is handled correctly.

### Physical

Any and all data stored physically is stored at a secure site with limited, controlled access. Documents containing personal information are stored within locked locations made accessible only to HIL staff who require them for a legitimate reason.

Any physical data that is to be disposed of is done so through a confidential document disposal service.

### Digital

Personal data stored digitally is either:

1. Stored locally on our private network
2. Stored remotely with a service provider

Any personal data that is stored digitally is subject to the same rules as our physical data. Our locally stored digital data is kept on a local server, accessible only to HIL staff who require them for a legitimate reason.

Any partner that stores data on behalf of Hethel Innovation Ltd must be audited to make sure they comply with the appropriate regulations.

### Partners that retain data on behalf of Hethel Innovation Ltd

All of our data partners are checked and audited to make sure they comply with the appropriate regulations as well as our internal policies. These partners are audited annually by the

* **Sendinblue** – Email marketing platform

<https://www.sendinblue.com/legal/privacypolicy/>

* **Godaddy** – Website hosting

<https://uk.godaddy.com/agreements/showdoc.aspx?pageid=PRIVACY>

* **Eventbrite** – Event management

<https://www.eventbrite.com/support/articles/en_US/Troubleshooting/eventbrite-privacy-policy?lg=en_US>

* **Zoho** – Customer relationship management

<https://www.zoho.com/privacy.html>

## Data retention timeframe

Where possible, personal data retained by Hethel Innovation Ltd will be erased after 18 months from the creation of the data or the last recorded interaction with that person.

However, Hethel Innovation Ltd has contractual obligations to retain all documentation relating to European Union funded activity for 25 years. This relates to personal information relating to people who have been provided support. In these cases, at the end of the project period (maximum 3 years after the data was created) digital data will be moved to physical storage media and securely archived with the relevant physical data.

In order to comply with European regulations, meet audit requirements and to avoid claw-back resulting from incomplete and unsatisfactory record-keeping, employees clearly label and store all records (original hard copies and/or electronic versions) in an easily accessible, secure place.

# Data use

Personal data is of no financial value to Hethel Innovation Ltd. 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.
* Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
* Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

# Data accuracy

The law requires Hethel Innovation Ltd 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 that 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.
* We will make it easy for data subjects to update the information the project holds about them. For instance, via the company website.
* 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.
* It is the marketing manager’s responsibility to ensure marketing databases are checked against industry suppression files every six months.

# Subject access requests

All individuals who are the subject of personal data held by Hethel Innovation Ltd are entitled to:

* Ask **what information** the company holds about them and why.
* Ask **how to gain access** to it.
* Be informed **how to keep it up to date.**
* Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company 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 privacy@hethelinnovation.com . The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 14 days.

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

# 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, Hethel Innovation Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company’s legal advisers where necessary.

# Providing information

The Breakthrough Project 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 company has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on the company’s website.