



Happy Business

Data Protection Policy

Date created: 13th February 2024

 hello@happy-business.co.uk

 www.happy-business.co.uk

Registered Office: Dove House Tregonigge Industrial Estate Falmouth TR11 4SU
Registered in England and Wales No: 14972753 VAT registration number: 448880742

1. Introduction

This policy is all about how Happy Business handles your information and respects the rights of our employees, customers, and partners under the law. When we talk about 'Data Protection Law,' we mean the rules in the United Kingdom that protect your privacy, like the UK GDPR, the Data Protection Act 2018, and other related laws.

In simple terms, this policy outlines how we collect, use, share, store, and get rid of your personal information. Everyone at Happy Business, including our employees, agents, contractors, and anyone else working with us, must follow the rules and principles mentioned here at all times.

2. Definitions

- **Consent:** This is when you agree to let us use your personal information. It has to be given freely, with clear information, and a positive action from you to show that you're okay with it.
- **Data Controller:** This is the person or organisation that decides why and how your personal information is used. In our case, Happy Business is the data controller for all personal data related to our staff, customers, partners and business contacts, used for our business purposes.
- **Data Processor:** This is a person or organisation that handles personal data on behalf of a data controller.
- **Data Subject:** This is you – a living person whose personal data we have.
- **EEA (European Economic Area):** This includes all EU Member States, Iceland, Liechtenstein, and Norway.
- **Personal Data:** Any information that can identify a person directly or indirectly, like a name, ID number, location data, or other specific details about someone.
- **Personal Data Breach:** When there's a security problem leading to accidental or unlawful loss, access, or disclosure of personal data.
- **Processing:** Any action we perform on personal data, like collecting, storing, or sharing, whether done manually or using machines.
- **Pseudonymisation:** Changing personal data in a way that it can't be linked to a specific person without using additional information.
- **Special Category Personal Data:** Extra-sensitive personal data, like details about race, political beliefs, health, etc.

3. Scope

3.1 Commitment to Fairness:

We are not just following the rules; we're committed to treating your personal data correctly, lawfully, and fairly. We respect everyone's legal rights, privacy, and trust.

3.2 Contacting Our Data Protection Officer:

If you have any questions about this policy or data protection laws, reach out to our Data Protection Officer, Beckie Pascoe, at beckie@happy-business.co.uk. They are in charge of making sure this policy is followed and developing related guidelines.

3.3 Responsibilities:

All directors, managers and associates must ensure that everyone working for us follows this policy. They need to put in place practices, processes, controls, and training to make sure we're doing things right.

3.4 When to Consult the Data Protection Officer:

Always get in touch with our Data Protection Officer in the following situations:

- If you are unsure about the legal basis for collecting, holding, or processing personal data.
- When relying on consent to collect, hold, or process personal data.
- If you are uncertain about how long to keep a particular type of personal data.
- When creating or updating privacy notices or similar documents.
- If you need help dealing with a data subject's rights or a subject access request.
- In case of a suspected or actual personal data breach.
- If you are unsure about the security measures needed to protect personal data.
- When sharing personal data with third parties.
- If transferring personal data outside the UK and have questions about the legal basis.
- Before starting significant new processing activities or making major changes to existing ones, requiring a Data Protection Impact Assessment.
- When using personal data for different purposes than originally collected.
- If there's any automated processing, including profiling or automated decision-making.
- For assistance in complying with the law related to direct marketing.

4. The Data Protection Principles

4.1 Fair and Transparent Processing:

We promise to handle your personal data fairly, lawfully, and transparently.

4.2 Specific and Legitimate Collection:

We will only collect your data for clear and legitimate reasons. We will not use it for anything else unless it is for important public, scientific, historical, or statistical purposes.

4.3 Just Enough Information:

We will only gather the data that's necessary for the reasons we told you about.

4.4 Accuracy and Timeliness:

We will make sure your data is accurate and, if needed, update it. If something is wrong, we will fix it quickly.

4.5 Limited Storage Duration:

We will keep your data for as long as needed for the reasons we collected it. If we need to keep it longer for public, scientific, historical, or statistical purposes, we will use extra measures to protect your rights.

4.6 Secure Processing:

We will keep your data safe from unauthorised or unlawful use, accidental loss, destruction, or damage. We will use the right technical and organisational methods to ensure its security.

These principles ensure that we follow the law and respect your rights. If you have any questions, feel free to ask our Data Protection Officer.

5. The Rights of Data Subjects under the UK GDPR

5.1 Right to Information:

You have the right to be informed about how and why we process your data.

5.2 Right of Access:

You can request access to the personal data we hold about you.

5.3 Right to Rectification:

If your data is incorrect, you can ask for it to be corrected.

5.4 Right to Erasure (Right to be Forgotten):

You have the right to request the deletion of your personal data.

5.5 Right to Restrict Processing:

You can limit how we use your data in specific circumstances.

5.6 Right to Data Portability:

You can obtain a copy of your data for your own use.

5.7 Right to Object:

You have the right to object to certain uses of your data.

5.8 Rights with Respect to Automated Decision-Making and Profiling:

If decisions about you are made by machines without human involvement, you can challenge them.

These rights, outlined in the UK GDPR, empower you to control and protect your personal data. If you have questions or want to exercise these rights, feel free to reach out to our Data Protection Officer.

6. Lawful, Fair, and Transparent Data Processing

6.1 Legal and Fair Processing:

We promise to process your personal data legally, fairly, and transparently, without harming your rights. The processing of personal data shall be lawful if at least one of the following applies;

- If you give us permission (consent).
- If it is necessary for a contract or before entering into one.
- If we have a legal obligation.
- If it is to protect someone's life.
- If it is for public tasks or official authority.
- If it is for our legitimate interests, but not if it harms your fundamental rights and freedoms, especially if you are a child.

6.2 Special Category Data:

If the data we are dealing with is sensitive, we will meet one of these conditions:

- If you explicitly agree, and the law allows it.
- If it is needed for employment, social security, or social protection laws, following the law or a collective agreement.
- If it is to protect someone's life and they cannot give consent.
- If we are a non-profit body with certain aims, and it is related to our legitimate activities.
- If you make your data public.
- If it is for legal claims or during court actions.
- If there is a substantial public interest and it is proportionate and respects your rights.
- If it is for health-related reasons, following the law and safeguards.
- If it is for public health, like protecting against serious health threats, following the law and safeguarding your rights.
- If it is for public interest, scientific research, or historical purposes, following the law and safeguarding your rights.

These rules make sure we are responsible and transparent in handling your data. If you have questions, contact our Data Protection Officer.

7. Consent

7.1 Clear Agreement:

Consent means you clearly agree to let us use your personal data. It could be a statement or an action on your part. Keeping quiet, pre-ticked boxes, or doing nothing will not count as consent.

7.2 Separate Consent:

If your consent is part of a document covering other things, the consent section must be kept separate.

7.3 Easy Withdrawal: You are free to change your mind and withdraw consent anytime. It should be simple for you to do so, and if you withdraw consent, we will act on it promptly.

7.4 New Purposes Require New Consent:

If we want to use your data for a different reason not originally told to you, we might need to ask for your consent again.

7.5 Special Category Data and Consent:

For sensitive data, we usually rely on other legal bases. If we do need your explicit consent, we will provide a clear privacy notice.

7.6 Keeping Records:

Whenever we rely on your consent, we will keep records to show we are following the rules. This ensures we can demonstrate our compliance with consent requirements.

If you have questions about your consent or want to withdraw it, please contact our Data Protection Officer.

8. Specified, Explicit, and Legitimate Purposes

8.1 What We Collect:

We gather personal data listed in Part 21 of this policy, directly from individuals and, if needed, from third parties.

8.2 Purposeful Collection:

We only collect, process, and keep personal data for the specific reasons mentioned in Part 21 or as allowed by Data Protection Law.

8.3 Keeping You Informed:

We make sure you always know why we're using your personal data. Check Part 15 for details on how we keep you informed.

9. Adequate, Relevant, and Limited Data Processing

9.1 Just Enough Information:

We only collect and process the data needed for the specific purposes we told you about in Part 8 and Part 21.

9.2 Job-Related Collection:

Our team collects personal data only necessary for their job and following this policy. We do not collect more than needed.

9.3 Job-Related Processing:

Personal data is only processed for reasons related to the job. No unrelated reasons are allowed.

10. Accuracy of Data and Keeping It Up-to-Date

10.1 Keeping Data Correct:

We make sure all personal data we have is accurate and up-to-date. If you want corrections, refer to Part 17.

10.2 Regular Checks:

We check data accuracy when collecting it and at regular intervals. If anything is wrong, we fix it promptly.

This ensures we collect, use, and maintain your data responsibly.

11. Data Retention

11.1 Keeping Data for What's Needed:

We will not keep your personal data longer than necessary for the reasons we collected it.

11.2 Disposing of Unneeded Data:

When we no longer need your data, we will get rid of it promptly.

11.3 Details in Data Retention Policy:

Check our Data Retention Policy for more on how long we keep specific types of personal data.

12. Secure Processing

12.1 Keeping Your Data Safe:

We make sure all your personal data is safe from unauthorised use, accidental loss, or damage. Check Parts 25 to 29 for details.

12.2 Regular Security Checks:

We regularly review and evaluate the measures we take to protect your data to ensure they stay effective.

12.3 Maintaining Data Security:

- Only authorised people who really need access can use your data.
- Your data must be accurate and suitable for its intended purpose.
- Authorised users should always be able to access the data they need for their authorised tasks.

13. Accountability and Record-Keeping

13.1 Responsibilities of Data Protection Officer:

Our Data Protection Officer is in charge of managing this policy and related guidelines.

13.2 Privacy by Design:

We always consider privacy when handling your data. If there's a significant risk, we conduct Data Protection Impact Assessments (refer to Part 14).

13.3 Employee Training:

All our team members get the right training on data protection, covering relevant laws, this policy, and other company policies.

13.4 Regular Compliance Checks:

We regularly review and evaluate our data protection compliance through Data Protection Audits.

13.5 Keeping Records:

We keep detailed records of our data collection, storage, and processing, including:

- Our company details and contacts.
- The reasons we collect, hold, and process your data.
- The legal basis for collecting, holding, and processing data.
- Categories of personal data and related data subjects.
- Details of any data transfers and security measures.
- How long we will keep your data (see our Data Retention Policy).
- Where we store your data.
- Technical and organisational measures we take to keep your data secure.

These measures ensure we handle your data responsibly and with accountability.

14. Data Protection Impact Assessments and Privacy by Design

14.1 Privacy by Design:

Whenever we start new projects or use new technologies involving personal data, we assess potential risks to your rights and freedoms.

14.2 Privacy by Design Principles:

We always consider privacy when handling your data. This includes:

- The nature, scope, context, and purpose of data handling.
- Current technical and organisational measures.
- Costs of implementing security measures.
- Risks to you and us, considering likelihood and severity.

14.3 Data Protection Impact Assessments (DPIAs):

Our Data Protection Officer oversees DPIAs, which cover:

- Types of personal data collected and processed.
- Purpose of data usage.
- Our objectives.
- How data is used.
- Parties consulted.
- Necessity and proportionality of data processing.
- Risks to you and us.
- Proposed measures to minimize risks.

15. Keeping Data Subjects Informed

15.1 Providing Information:

We share the following information with you:

- If we collect data directly from you, we tell you the purpose at collection.
- If we get data from a third party, we inform you:
 - When we first communicate with you.
 - Before transferring data to another party.
 - Within one month of obtaining the data.

15.2 Privacy Notice Contents:

We provide a privacy notice containing:

- Our details and contacts, including our Data Protection Officer.
- Purpose and lawful basis for collecting and processing data.
- Legitimate interests if applicable.
- Categories of collected data if obtained indirectly.
- Details of third parties receiving the data.
- Data transfers outside the UK and safeguards (refer to Part 31).
- Applicable data retention periods.
- Your rights under the UK GDPR.
- Your right to withdraw consent.
- Your right to complain to the Information Commissioner's Office.
- Source of data if not obtained directly.
- Legal or contractual requirements for data collection and consequences of non-provision.
- Details of any automated decision-making or profiling, including how decisions are made and their consequences.

This ensures transparency and keeps you informed about how we handle your data.

16. Data Subject Access

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which Happy Business holds about them, what it is doing with that personal data, and why.

Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All SARs received shall be handled by Happy Business's Data Protection Officer.

17. Rectification of Personal Data

Data subjects have the right to require that Happy Business rectify any of their personal data that is inaccurate or incomplete.

Happy Business shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing us of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

18. Erasure of Personal Data

18.1 When You Can Ask for Data Deletion:

You have the right to request the removal of your personal data in the following situations:

- It is no longer needed for the original purpose.
- You withdraw your consent for us to hold and process your data.
- You object to us holding and processing your data, and there's no overriding reason.
- The data has been processed unlawfully.
- Erasure is needed for us to comply with a legal obligation.

18.2 Timely Response to Your Request:

We will generally erase your data within one month of receiving your request. If it is a complex request, we might extend this by up to two months, and we will let you know if we need more time.

18.3 Informing Third Parties:

If your data has been shared with others and we erase it upon your request, we will inform them too, unless it is impossible or requires disproportionate effort.

19. Restriction of Personal Data Processing

19.1 Asking Us to Stop Processing:

You can request us to stop processing your personal data. If you do, we will keep only the necessary data to ensure it is not processed further.

19.2 Informing Third Parties about Restrictions:

If your data has been shared with others and we restrict processing upon your request, we will inform them too, unless it is impossible or requires disproportionate effort.

20. Direct Marketing

20.1 Marketing Rules:

When promoting our services, Happy Business follows specific rules and regulations.

20.2 Consent for Electronic Direct Marketing:

For electronic direct marketing, such as emails and text messages, we generally require prior consent from data subjects.

However, there is a limited exception:

We may send marketing text messages or emails to a customer if their contact details were obtained during a sale, the marketing relates to similar products or services, and the customer had the chance to opt-out when their details were first collected and in every subsequent communication.

20.3 Offering the Right to Object:

We explicitly offer the right to object to direct marketing in a clear and understandable way. This option is kept separate from other information to ensure clarity.

20.4 Responding to Objections:

If a data subject objects to direct marketing, we promptly comply with their request

21. Personal Data Collected, Held, and Processed

Happy Business collects, holds, and processes the following personal data. For information on data retention, please refer to Happy Business's Data Retention Policy:

Type of Data	Purpose of Data
Your contact details	To manage our internal client database (CRM) and to maintain contact with you for marketing purposes or other commercial purposes
Your communication data	To manage our internal client database (CRM) and to maintain contact with you for marketing purposes or other commercial purposes
Your use of our services	Information relating to your use of our Services
Your financial details	Financial information disclosed to us which can be linked to you as a client or supplier, such as bank account details or invoicing details
Webinar recordings and recordings of other events	When you attend webinars or other events hosted by us, we may make sound and/or video recordings and or take photos. We will inform you beforehand if this is the case and you can choose to opt out of these recordings and photos.
Any other Personal Data	Any other Personal Data which you choose to disclose to us during the course of your contractual relationship with us.

22. Data Security - Transferring Personal Data and Communications

We take special care when handling your personal information. Here's what we do to keep it safe during communication and transfers:

- **Encrypting Emails:** We use special protection for emails with your personal data to keep it safe.
- **Confidential Marking:** Any emails containing your personal data are marked as "confidential."

- **Secure Networks Only:** We only send your personal data over secure networks, never over unsecured ones.
- **Prefer Wired Networks:** If there's a secure wired option, we avoid sending personal data over wireless networks.
- **Safe Handling of Email Content:** If your personal data is in an email, we copy it to a secure location, delete the email, and remove any associated temporary files.
- **Direct Transfer of Hard Copies:** When transferring personal data in hardcopy form, we hand it directly to the recipient or use a reliable delivery service.

23. Data Security - Storage

We ensure that your personal data stays safe when stored. Here's how:

- **Electronic Copies:** Digital copies of your personal data are stored securely with passwords for added protection.
- **Hardcopies and Removable Media:** If we transfer physical copies, they will be kept in a locked box, drawer, or cabinet. Electronic copies on removable media follow the same secure storage.
- **Regular Backups:** We back up electronic personal data regularly. All backups are encrypted for extra security.
- **No Mobile Storage:** We don't store personal data on mobile devices unless approved in writing. If approved, it follows strict guidelines and is kept for the minimum necessary time.

24. Data Security - Disposal

When we need to get rid of personal data, we do it securely. Whether it is erasing electronic files or disposing of physical copies, we ensure it is done properly. For more details, check out Happy Business's Data Retention Policy.

25. Data Security - Use of Personal Data

To make sure your personal data is handled responsibly, we follow these measures:

- **Formal Access Requests:** No personal data is shared casually. If someone needs access, they formally request.
- **Authorised Transfers:** Personal data does not move between employees, agents, contractors, and anyone else we are working with without approval from the data processor or data controller.
- **Handle with Care:** We take care of personal data, making sure it is never left unattended or visible to unauthorised eyes.
- **Computer Security:** If personal data is on a computer screen, and the computer is left alone, the user must lock it for security.
- **Marketing Responsibility:** If personal data is used for marketing, the marketing director ensures proper consent and respects opt-outs, like those registered with services such as TPS.

26. Data Security - IT Security

When it comes to IT and information security, we take these steps:

- **Password Protection:** Passwords for personal data are changed regularly, using a mix of letters, numbers, and symbols.
- **No Sharing Passwords:** Passwords are never shared or written down. If forgotten, they must be reset following the proper procedure.
- **Software Updates:** All software, including applications and operating systems, is kept up-to-date by Happy Business's IT staff to ensure security.
- **Approved Software Only:** No new software can be installed on Company-owned devices without approval from our IT solutions provider.

27. Organisational Measures

We ensure everyone involved knows their responsibilities when it comes to personal data. Here's how:

- **Awareness and Training:** All employees, agents, contractors are educated about their responsibilities under Data Protection Law and this Policy.
- **Need-to-Know Access:** Only those who need personal data for their duties have access to it.
- **Compliance with Sharing:** Sharing of personal data adheres to what's communicated to data subjects, with their consent if necessary.
- **Continuous Training:** Everyone handling personal data is regularly trained to do so responsibly.
- **Confidentiality:** Everyone involved is encouraged to be cautious and discreet when discussing work-related matters related to personal data.
- **Periodic Reviews:** Personal data held by Happy Business is periodically reviewed, as outlined in Happy Business's Data Retention Policy.
- **Contractual Obligations:** All involved parties are contractually bound to follow Data Protection Law and this Policy.

28. Transferring Personal Data to a Country Outside the UK

We sometimes need to transfer personal data to countries outside the UK, but we take steps to ensure your data stays protected. Here's how:

- **Adequacy Decisions:** We only send your data to countries with strong data protection rules, making sure your information gets the same protection as it would here.
- **Your Consent:** If you have given us explicit consent, we may transfer your data.
- **Other Legitimate Reasons:** Data may be transferred for reasons like fulfilling a

contract, public interest, legal claims, protecting vital interests, or, in limited cases, for our legitimate interests.

29. Data Breach Notification

We take data breaches seriously and have a process in place:

- **Immediate Reporting:** Any suspected or confirmed data breaches must be reported right away to our Data Protection Officer.
- **Informing Authorities:** If a breach poses a risk to your rights and freedoms, we notify the Information Commissioner's Office within 72 hours.
- **Direct Communication:** If the breach poses a high risk, we inform you directly and promptly.
- **Notification Details:** Our breach notifications include information about the affected individuals, the data records involved, our Data Protection Officer's contact details, likely consequences of the breach, and the measures taken to address it.

These measures ensure we handle data breaches transparently and take necessary actions to protect your information.

This Policy has been approved and authorised by:

Name: Beckie Pascoe

Position: Operations Director

Date: 13th Feb 2024

Due for review: 13th Feb 2025