



General Data Protection Regulation (GDPR) Policy

Document Ref	Author	Approved by	Signature	Last review date
POL040	Mhairi Shields	Mhairi Shields		24 August 2026

Contents

1. Introduction	3
2. Scope.....	3
3. Other policies to consider	3
4. Key definitions.....	3
5. Data Protection Manager (DPM).....	4
6. Data protection principles	5
7. Lawfulness, transparency, and fairness of processing data	5
7.1 Lawful processing of personal data	5
7.2 Lawful processing of sensitive personal data	5
7.3 Consent to processing	6
7.4 Transparency	6
8. Collection and retention of data	7
8.1 Collection of data	7
8.2 Accuracy of data	7
8.3 Purpose limitation	7
8.4 Retention of data.....	7
9. Data security and sharing	7
9.1 Data security	7
9.2 Record keeping.....	8
9.3 Data sharing	8
9.4 Automated processing and decision-making (including profiling)	8
9.5 Direct marketing.....	9
9.6 Transfer of data outside the EU	9
10. Data subject rights.....	9
11. Compliance with policy.....	10
11.1 Data security breaches	10
11.2 Privacy by design and Data Protection Impact Assessment (DPIA)	10
12. Data protection complaints	10
13. Training	11
14. Breaches of this policy	11
15. Policy review	11

1. Introduction

Venesky Brown is committed to being transparent about how it collects and uses the personal data of our workforce, customers, suppliers, and other third parties, and to meeting its data protection obligations. We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.

This policy applies to all personal data we process, regardless of the media on which that data is stored or whether it relates to past or present employees, workers, subcontractors (including any substitutes and/or hired assistants, where applicable) customers, clients or supplier contracts, shareholders, website users or any other data subject.

All Directors and the Data Protection Manager (DPM) are responsible for ensuring all the Company workforce comply with this policy and will ensure appropriate practices, processes, controls and training are implemented to ensure such compliance.

2. Scope

This policy applies to all Venesky Brown employees (current and former), agency staff, workers, subcontractors and Limited Company Contractors.

This policy does not form part of your contract of employment except to the extent that it imposes obligations on you. We may amend this policy at any time and may vary it as appropriate to a particular case.

3. Other policies to consider

You should read this policy in conjunction with the following policies:

- GDPR Privacy Notice
- Data Retention Policy
- Complaints Policy
- Whistleblowing Policy
- Code of Conduct
- Disciplinary Policy and Procedure

4. Key definitions

Key definitions used throughout this policy include:

Data Controller	The person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with GDPR. Venesky Brown is the data controller of all personal data relating to our company workforce and personal data used in our business for our own commercial purposes.
Data Subject	A living, identified, or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Personal Data	Information about a living individual from which they can be identified (or from which they can be identified along with other information we hold or can reasonably access). This information can be stored in any media (e.g. paper or a computer database). Some examples are: • Personal contact details, such as name, address, email, telephone number. • Date of birth. • Bank account details. • Opinion about a person's actions or behaviour, for example, expressed in an email or interview notes. Personal information can relate to, for example, past or present employees, workers, contractors, customers, clients, suppliers, shareholders, website users, or members of the public. Personal information does not include data where the identity has been removed (anonymised data).
Special Categories of Personal Data	Information about an individual's racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sex life or sexual orientation; criminal convictions; offences or alleged offences; genetic data; or biometric data for the purpose of uniquely identifying an individual.
Processing	Any activity that involves using personal information. This includes collecting, recording, storing, retrieving, using, amending, disclosing it, and transferring it to third parties.
Privacy Notices	Separate notices setting out information that may be provided to data subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals e.g. employee privacy notices or the website privacy notice, or they may be standalone, one-time privacy statements covering processing related to a specific purpose.
Data Privacy Impact Assessment (DPIA)	Tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the processing of personal data.
Automated Processing	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.
Automated Decision-Making	When a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

5. Data Protection Manager (DPM)

We have appointed a Data Protection Manager (DPM). If you have any questions about this policy or your data protection obligations, please contact Mario Holligan at mario@venesky-brown.co.uk

6. Data protection principles

When processing personal information, we adhere to the following data protection principles. Personal information must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected only for specified, explicit and legitimate purposes, and processed only in line with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- 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.
- 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, using appropriate technical or business measures.

7. Lawfulness, transparency, and fairness of processing data

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, lawfully, and for specified purposes. The GDPR restricts our action regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but to ensure that we process personal data without adversely affecting the data subject.

The GDPR allows processing of personal data for specific purposes, some of which are set out below:

7.1 Lawful processing of personal data

Personal information will only be processed when there is a lawful basis for doing so. Most commonly, the Company will use personal information in the following circumstances:

- When it is needed to perform employee's contracts of employment.
- When it is needed to comply with a legal obligation.
- To pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable Privacy Notices, or you must identify and document the legal ground being relied on for each processing activity in accordance with the Company's guidelines on lawful basis for processing personal data.

The Company may also use personal information in the following situations, which are likely to be rare:

- When it is necessary to protect the data subject's vital interests.
- When it is necessary in the public interest or for official purposes.

7.2 Lawful processing of sensitive personal data

The Company will process special categories in the following circumstances:

- In limited circumstances, with explicit written consent.
- In order to meet legal obligations.
- When it is needed in the public interest, such as equal opportunities monitoring.
- When it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, the Company may process this type of information where it is needed in relation to legal claims or where it is needed to protect an employee's interests (or someone else's interests) and the employee is not capable of giving consent, or where an employee has already made the information public. We may use particularly sensitive personal information in the following ways:

- Information relating to leaves of absence, which may include sickness absence or family related leaves, may be used to comply with employment and other laws.
- Information about an employee's physical or mental health, or disability status, may be used to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- Information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, may be used to ensure meaningful equal opportunity monitoring and reporting.
- Information about trade union membership may be used to pay trade union premiums, register the status of a protected staff member and to comply with employment legislation.

7.3 Consent to processing

A data controller must only process personal data on the basis of one or more of the lawful basis set out in the GDPR, which includes consent.

A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

Unless we can rely on another legal basis for processing, consent is usually required for processing sensitive personal data, for automated decision-making and for cross border data transfers. We will usually rely on another legal basis to process most types of sensitive data. Where consent is required, you must issue a Privacy Notice to the data subject to capture consent.

You will need to evidence consent captured and keep records of all consents so the Company can demonstrate compliance as required.

7.4 Transparency

The GDPR requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or elsewhere. Such information must be provided through appropriate privacy notices which are concise, transparent and easily accessible for data subjects.

Whenever we collect personal data directly from data subjects, our privacy notices must identify the data controller and DPM, how and why we will use, process, disclose, protect and retain personal data. The privacy notice must be presented to the data subject when they first provide their personal data.

When personal data is collected indirectly (for example, from a third party or publicly available source), you must provide the data subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

8. Collection and retention of data

8.1 Collection of data

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You may only collect and process personal data where performing the duties of your role requires it. You must ensure that you do not collect excessive data and when personal data is no longer needed for the specified purposes, it is deleted or anonymised in accordance with the Company's Data Retention Policy.

8.2 Accuracy of data

You will ensure the personal data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

8.3 Purpose limitation

Personal data must be collected only for specified, explicit and legitimate 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 they have consented where necessary.

8.4 Retention of data

We will only retain personal information for as long as necessary to fulfil the purposes it was collected for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of personal information are set out in the Data Retention Policy.

When determining the appropriate retention period for personal data, we will consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which personal data is processed, whether the Company can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise personal information so that it can no longer be associated with individual employees, in which case we may use such information without further notice to employees. After the data retention period has expired, the Company will securely destroy employee personal data.

9. Data security and sharing

9.1 Data security

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

All employees are responsible for protecting the personal data we hold. You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third party service providers who agree to comply with the required policies and procedures, and who agree to put adequate measures in place, as requested.

Data security must be maintained by protecting the confidentiality, integrity and availability of the personal data. You must comply with and not attempt to circumvent the administrative, physical, and

technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

9.2 Record keeping

The GDPR requires us to keep full and accurate records of all our data processing activities.

You must keep and maintain accurate corporate records (including for our external contractors) reflecting our processing including records of data subjects' consents and procedures for obtaining consents in accordance with the Company's guidelines.

These records should include, at a minimum, the name and contact details of the data controller and the DPM, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, personal data retention periods and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

9.3 Data sharing

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the personal data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the personal data we hold with third parties, such as service providers if:

- They have a need to know the information for the purposes of providing the contracted services.
- Sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained.
- The third party has agreed to comply with the required data security standards, policies and procedures, and put the adequate security measures in place.
- The transfer complies with any applicable cross border transfer restrictions.
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

9.4 Automated processing and decision-making (including profiling)

We do not currently engage in automated processing or decision-making. However, if this should change you must comply with the Company's guidelines.

Generally automated-decision making is prohibited when a decision has a legal or similar significant effect on an individual.

If a decision is to be based solely on automated processing (including profiling), a data impact assessment (DPIA) must be carried out before any activities are undertaken. The data subjects must then be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. The data subject must also be informed of the logic involved in the decision making or profiling, the significance and envisaged consequences and provide the data subject the right to request human intervention, express their point of view or challenge the decision.

9.5 Direct marketing

We do not currently engage in direct marketing. However, should this change, you must comply with the Company's guidelines.

A data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject and presented clearly and separately from other information. A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be updated to include just enough information to ensure marketing preferences are respected in future.

9.6 Transfer of data outside the EU

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data across borders when you transmit, send, view or access that data in, or to, a different country.

You may only transfer personal data outside the EEA if one of the following conditions apply and you must comply with the Company's guidelines on cross border data transfers:

- The European Commission has issued a decision confirming the country to which we transfer the personal data ensures an adequate level of protection for the data subject's rights and freedoms.
- Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPM.
- The data subject has provided explicit consent to the proposed transfer after being informed of any potential risks.
- The transfer is necessary for one of the other reasons set out in the GDPR and detailed in Section 7.

10. Data subject rights

Data subjects have rights when it comes to how we handle their personal data, including:

- Receive certain information about our processing.
- Request access to their personal data that we hold (often known as a "subject access request").
- Request transfer, correction, deletion, or restriction of processing.
- Object to processing (including where this is for direct marketing).
- Request a copy of an agreement transferring personal data outside of the EEA.
- Object to decisions based solely on automated processing, including profiling.
- Be notified of a personal data breach.
- Complain to the Information Commissioner.
- Withdraw their consent to processing (if we process their personal data on the basis of their consent).

The identity of the individual requesting data under any of the rights listed above must be verified (do not allow third parties to persuade you into disclosing personal data without proper authorisation). If you receive any communication that appears to relate to these rights, you must contact the DPM immediately. Do not respond to the communication or attempt to deal with it without input from the DPM.

11. Compliance with policy

11.1 Data security breaches

We are required to notify the applicable regulator and, in certain instances, the data subject of any personal data breaches.

We have procedures in place to deal with any suspected data breaches and will notify data subjects or any applicable regulator where we are legally required to do so. If you know or suspect a data breach has occurred, do not attempt to investigate the matter yourself, you should immediately contact the DPM. You should preserve all evidence relating to the potential data breach.

11.2 Privacy by design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when processing personal data by implementing appropriate and effective technical and organisational measures, to ensure compliance with data privacy principles. You must comply with the Company's guidelines on DPIA and Privacy by Design.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

- The state of the art
- The cost of implementation.
- The nature, scope, context and purposes of processing.
- The risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

Data controllers must also conduct DPIAs in respect to high-risk processing. You should conduct a DPIA (and discuss your findings with the DPM) when implementing major system or business change programs involving the processing of personal data including:

- Use of new technologies or changing technologies (programs, systems or processes).
- Automated processing including profiling and automated decision-making.
- Large scale processing of sensitive data.
- Large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- A description of the processing, its purposes and the data controllers' legitimate interests if appropriate.
- An assessment of the necessity and proportionality of the processing in relation to its purpose.
- An assessment of the risks to individuals.
- The risk mitigation measures in place and demonstration of compliance.

12. Data protection complaints

Under the UK GDPR and the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025), individuals have the right to complain to Venesky Brown if they believe we have infringed their data protection rights or mishandled their personal data.

If you receive a complaint of this nature, or if an individual raises a concern about how their personal data has been handled, you should direct them to raise this in the first instance by phone on 0131 357 2140, so that we can try to resolve the matter informally.

If the individual remains unsatisfied following this informal stage, they should be directed to our Quality Manager, Lindsey Gatherer, who can be contacted at lindsey@venesky-brown.co.uk. All data protection complaints must be handled in line with our Complaints Policy, which sets out the full process, including timescales for acknowledgement and investigation.

Individuals should also be informed that they retain the right to complain to the Information Commissioner's Office (ICO) at any stage.

13. Training

The Company will provide ongoing mandatory training to its workforce to enable them to comply with data privacy laws.

14. Breaches of this policy

If you think you may have breached this policy, please speak to your line manager or the DPM as soon as possible. Quick action can be crucial in mitigating the effects of a breach.

Breaches of this policy may be dealt with under our Disciplinary Policy and, in serious cases, may be treated as gross misconduct leading to dismissal without notice.

15. Policy review

This policy will be monitored by the HR team and will be reviewed annually. It may also be reviewed in the light of experience gained from its operation, advice obtained from reputable sources, and changes in legislation or regulation.