

Data Protection Policy

Amendment History

Modified Date	Modifier	Version	Modification Reason	Approved By	Date
12/12/23	CF, IT Risk & Compliance Officer	1.0	Initial Version	RA, Head of Information Security	02/05/24
10/02/25	JM, Internal Audit Experienced Senior	1.1	Minor tweaks to language and further extension to third parties.	CTH, Head of Regulatory Compliance	10/02/25
31/07/26	JM, Internal Audit Experienced Senior	1.2	Amendments to language to cover external parties	CTH, Head of Regulatory Compliance	31/07/26
17/08/2026	CTH, Head of Regulatory Compliance	2.0	Restructure and further detail around legal principles	AR, Legal Director	02/09/26

Last reviewed: September 2026

Document Scope

Focused Consulting Limited ("Focused") is part of the PayStream group of companies, of Mansion House, Manchester Road, Altrincham, WA14 4RW. Whilst Focused is the entity which employs umbrella contractors to work on temporary assignments for external third parties, PayStream Accounting Services Limited ("PAS") is the entity which employs internal staff to operate the running of the business and for making decisions as to the data we collect from employees and how such data is processed.

This policy sets out how PAS and its group companies ("we", "us", or "the Company") collect, use, store and share personal data in connection with the services we provide.

It explains both:

- how we handle personal data; and
- the standards and behaviour expected of our employees, contractors, subcontractors and supplier staff ("you") when accessing, using or sharing any personal data (including data relating to agency staff, end clients, subcontractors or other third parties), whilst working for us, or on our behalf.

This policy applies in addition to any other contractual or legal obligations that apply to you.

Responsibilities

Company Privacy Team:

The Privacy Team has direct responsibility for procedures relating to the protection of data, including Subject Access Requests. The team is responsible for reviewing the details of potential or actual breaches of personal data notifications to ensure that, where necessary, these are referred back to the ICO. Additional requirements for notification may also arise from Personal Data Impact Assessments.

A record of any notification to the ICO will be retained by the Privacy Team. The ICO website guidance is used as the authoritative guidance for notification. Any relevant notifications are reviewed and updated notifications are issued accordingly.

IT Staff (of the Company and where relevant, the End Client):	Responsible for ensuring that data protection technical controls are implemented and records maintained.
Company employees, contractors, subcontractors and supplier staff	Responsible for ensuring that data protection controls are followed and for notifying the Privacy Team of concerns or breaches of personally identifiable information (PII). This includes following the controls of external companies and those of end clients, where any individual is engaged to provide services to third parties All staff employed or engaged by the Company, including those employed or engaged by its group umbrella companies, are responsible for ensuring that personal data supplied by them is accurate and up to date.
Management:	Responsible for ensuring that employees, contractors, subcontractors and supplier staff comply with this Policy.

Introduction

The Company needs to collect and use certain types of personal information about staff and other individuals who come into contact with the Company in order to operate. This includes, for example, internal staff employed or engaged by PayStream Accounting Services Limited (“Internal Company Staff”), employees, subcontractors, agency staff, and external suppliers. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

You may also be granted access to such personal data during your employment or engagement with us when you carry out work for us, or on our behalf.

All external suppliers, third parties, organisations, employees or individuals working with or for the Company, or, on our behalf, who have access to personal information will be expected to comply with this policy. You must also comply with any policies operated by our clients, for example, where you are working off-site at another company’s business, or within their systems.

In all cases, personal information must be dealt with properly, however it is collected, recorded and used (whether on paper, in a computer, or recorded on other material) and safeguards must be put in place to ensure this is within the scope of the [UK General Data Protection Regulation](#), the [Data Protection Act 2018](#) and, where applicable, the [EU General Data Protection Regulation](#) (together, the “Data Protection Legislation”).

The Company’s Senior Management is strongly committed to the rights of individuals whose data they collect and process and ensure that the Company complies with the objectives and obligations of all applicable laws related to personal information and that controls are in place that reflect the level of risk that the Company is willing to accept.

The Company takes steps to ensure that it is able to meet all the regulatory, statutory and contractual obligations that are applicable, including the protection of the interests of individuals and other stakeholders.

We expect the same standards to be upheld by you when processing personal data whilst carrying out work for, or on behalf of, the Company.

Monitoring technologies may be implemented to detect and assist in the prevention of unauthorised activities. The technologies implemented must be relevant, used appropriately, and be limited to the minimum necessary to meet the above objectives in alignment with relevant regulations.

Any breach of the Data Protection Legislation and/or this policy, may be considered a breach of the Company’s Disciplinary Policy (where applicable) and a breach of contract. Depending on the circumstances, it may also be considered a criminal offence, potentially resulting in prosecution.

Data Protection Principles

Any processing of personal data must be conducted in accordance with the data protection principles of the Data Protection Legislation, as outlined below.

Lawfulness, Fairness, and Transparency

Personal data must be processed lawfully, fairly and transparently, avoiding misuse or unexpected processing, with clear communication to individuals about how their data is used.

For every instance of processing personal data, there must be at least one lawful basis identified before the processing begins, such as consent, contract, legal obligation, vital interests, public task, legitimate interests or recognised legitimate interests.

Before relying on legitimate interests as the applicable lawful basis, we will document a Legitimate Interest Assessment (LIA) to assess the purpose and necessity to ensure a lawful interest exist. The processing must be found necessary, and individuals' rights must not be overridden prior to proceeding.

Where it is deemed necessary, consent to process personal and sensitive data must be obtained using standard consent documents. This may for example, be through a contract of employment or during initial induction.

'Consent' is taken by the Company to mean that agreement to the processing of personal data has been explicitly and freely given and that this consent is specific, informed and an unambiguous indication of the data subject's wishes. The consent of the data subject can be withdrawn at any time.

Consent is also taken by the Company on the basis that it has been given by the data subject who is fully informed of the intended processing and is in a fit state of mind and without undue pressure to give consent being applied. There must be some active communication between the parties which demonstrates active consent (i.e., it cannot be inferred from non-response to a communication). For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

The UK GDPR includes requires transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' 'rights and freedoms'.

Information must be communicated to the data subject in an intelligible form using clear and plain language.

The way in which the Company processes data is outlined clearly in our privacy notices, which are shared at the start of each employment or engagement with the relevant individual, within the footer of each email we send and on our website.

Purpose Limitation

Data should be collected for specified, explicit, and legitimate purposes and not used in ways incompatible with those purposes. Exceptions exist for archiving, research, or statistical purposes, provided safeguards are in place.

The purposes the Company uses data for are documented in our Records of Processing Activities and communicated to data subjects through our Privacy Notices.

Personal data relating to employees, umbrella employees, CIS contractors, agency staff, end clients, subcontractors, customers and other third parties will only be used:

- to deliver our services and perform our contractual obligations;
- to meet our legal and regulatory obligations (including tax, employment, anti-money laundering and other compliance requirements); and
- for other purposes that are compatible with those original purposes and within the reasonable expectations of the data subjects.

Personal data for new, unrelated purposes must not be used without first:

- identifying and documenting the new purpose;
- confirming a suitable lawful basis for the processing; and
- updating relevant Privacy Notices and, where required, obtaining fresh consent.

All staff, including employees, contractors, subcontractors and supplier staff working for or on behalf of the Company, must ensure that personal data is only accessed and used for authorised business purposes and must not repurpose personal data for personal use or any unrelated activity. Any proposed new use of existing personal data by the Company must be referred to the Privacy Team before it is implemented.

Data Minimisation

Only data that is adequate, relevant, and necessary for the intended purpose should be collected. This principle prevents excessive or irrelevant data collection.

The Company will:

- identify the minimum personal data required for each processing activity and ensure that our systems, forms and processes do not request more data than is needed;
- avoid collecting personal data “just in case” it may be useful in future; and
- regularly review the personal data we hold to ensure it remains necessary and proportionate for our stated purposes.

All staff working for or on behalf of the Company, including but not limited to umbrella/PEO employees, CIS contractors and supplier staff, must ensure that they do not collect or retain unnecessary personal data and must follow the Company’s data collection standards, templates and retention rules. Any concerns about excessive data collection must be raised with the Privacy Team.

Accuracy

Personal data must be accurate and kept up to date. Reasonable steps must be taken to correct or erase inaccurate data without delay

The Company’s Management is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it. Through appropriate training, staff are aware of their responsibility for ensuring that all necessary actions are taken to ensure personal information is accurate and up to date. This should also take into account the volume of data collected, the speed with which it might change and any other relevant factors.

All individuals in scope of this policy are responsible for ensuring that any data held by the Company is accurate and up to date. Any data submitted by an individual to the Company, such as via a registration form, will be considered to be accurate at the time of receipt. Employees or other individuals should notify the Company of any changes in personal information to ensure personal information is kept up to date. It is the responsibility of the Company to ensure that any notification of changes to personal information is implemented.

If a third party has provided inaccurate or out-of-date personal information, the staff member who identifies this is responsible for informing them that the personal information is inaccurate and/or out-of-date and will advise them that the information should no longer be used. The relevant staff member should also ensure that any correction to the personal information is passed on to the third party in an appropriate and secure manner.

Storage Limitation (Data Retention, Deletion and Disposal)

Data should be kept only as long as necessary for the purposes it was collected. Longer storage is allowed for research or archiving if appropriate safeguards are implemented.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing and personal data must not be retained for longer than it is required. It is expected that you will not

access, process or store personal data in connection to your particular role for or on behalf of the Company, for any longer than is necessary.

Once it is no longer required for the purposes it was collected, personal data must be deleted and/or disposed of in a way that protects the 'rights and freedoms' of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion, or obfuscation of personally identifiable data).

Some data will be kept for longer periods than others. Data held by the Company is deleted in accordance with the Company's internal Information Classification and Data Retention Directives and, once its retention date is passed, it must be securely destroyed.

Principles for deletion of records held on cloud services are identical to non-cloud records.

The Company implements automated data clean-ups according to the business' agreed criteria. Our Internal Audit function within our Regulatory Compliance team, carry out regular checks to ensure any data that is no longer required in the context of the original purpose is appropriately removed and securely disposed of, as expected in line with our auto-data retention script. Further, we hold regular data protection meetings to discuss the Company's approach to data across the business and any upcoming changes to processing.

The Company's Management review at least annually personal data processed in connection with their departments and destroy data no longer required.

Integrity and Confidentiality (Data Security)

Appropriate technical and organisational measures must be put in place to protect data against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personal data should be accessible only to those who need to use it and must be processed in a manner that ensures its security.

The Company's compliance with this principle is contained within its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001:2022 and the Security Policy set out in the ISMS.

The controls the Company has in place have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to audit and review.

All individual responsible for any personal data must keep it securely and ensure that it is not disclosed under any conditions to any third party unless that third party has been specifically authorised to receive that information and, where necessary, has entered into a confidentiality agreement. Third parties who require access to personal data must agree to confidentiality provisions (either within a confidentiality agreement, contractual document or otherwise) before access is permitted. It is expected that such agreements should include the right for the Company to audit compliance with such provisions.

You should form a judgment based upon the sensitivity and value of the information in question. As appropriate, personal data must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, it must be password protected. In the case of Internal Company staff passwords must be in line with the Access Control Aspects and Secure Systems & Development Aspects Directives. In the case of other employees, contractors, subcontractors or supplier staff complex passwords should be used. We recommend passwords (including those used to gain access to remote desktops, computer systems and our app and portal, where relevant) are set with a minimum of 15 characters, in line OWASP recommendations. You must also comply with any applicable end client requirements in this regard; and/or

- Stored on encrypted removable media. In the case of internal Company staff, this must be in line with the Cryptography Aspects Directive

Care must be taken to ensure that PC screens and terminals are not visible except to authorised staff. Internal Company Staff must review the Company's Acceptable Use Aspects Directive before accessing Company information.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit (written) authorisation.

As soon as manual records are no longer required, the Company will remove these from secure archiving. Manual records that have reached their retention date are shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are removed and immediately destroyed.

Personal data shall not be transferred to a country or territory outside the UK and EEA unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the UK and EEA is prohibited unless one or more of the specified safeguards or exceptions apply, taking into account the following factors:

- The nature of the information being transferred;
- The country or territory of the origin, and final destination, of the information;
- How the information will be used and for how long;
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- The security measures that are to be taken as regards the data in the overseas location.

The Company ensures that personal data is not disclosed to unauthorised third parties including family members, friends, government bodies and, in certain circumstances, the police unless it has a lawful basis to do so.

UK GDPR permits a number of exemptions where certain disclosure without consent is permitted, as long as the information is requested for one or more of the following purposes:

- To safeguard national security;
- Prevention or detection of crime including the apprehension or prosecution of offenders;
- Assessment or collection of tax duty;
- Discharge of regulatory functions (includes health, safety and welfare of persons at work);
- To prevent serious harm to a third party; and
- To protect the vital interests of the individual - this refers to life and death situations. Requests to provide data for one of these reasons must be supported by appropriate paperwork.

All employees, and other individuals engaged by the Company, should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not a disclosure of the information is relevant to, and necessary for, the conduct of business operations.

Accountability

The Company may act as either a data controller and/or a data processor, as defined under the UK GDPR and the Data Protection Act 2018, depending on the nature of the processing.

The UK GDPR states that data controllers are responsible for ensuring compliance and for demonstrating that each processing operation complies with the requirements of the UK GDPR.

Where the Company acts as a data controller, we keep all necessary documentation of all processing operations and implement appropriate security measures. We are also responsible for completing Data Processing Impact Assessments (DPIAs), complying with requirements for prior notifications, or approval from supervisory authorities

and ensuring a Data Protection Officer is appointed, where required. Our Data Protection Officer is Legal Director, Alison Roberts.

To ensure that the Company is aware of any risks associated with the processing of all types of personal information, a risk assessment has been implemented to assess risk to individuals during the processing of their personal information.

Where the processing of personal information may result in a high risk to the 'rights and freedoms' of natural persons, a Data Protection Impact Assessment ("DPIA") must be completed prior to conducting the processing, to ensure the personal information is protected. This assessment may also be used to apply to a number of similar processing scenarios with a similar level of risk.

Where, as a result of a DPIA, it is clear that the Company will process personal information in a manner that is likely to result in a high risk to the 'rights and freedoms' of the data subjects, the Privacy Team review the process before the Company proceeds. If there are significant risks to the data subject the team will escalate to the Privacy Team, and if necessary, the ICO for final guidance.

Data Subjects' Rights

Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To be informed about the collection and use of their personal data;
- To make subject access requests regarding information held about them in electronic format and manual records which form part of a relevant filing system and to whom such data has been disclosed. This includes the right to inspect confidential personal references and information obtained from third parties about that person. When received by the Company, such requests are reviewed and responded to by the Privacy Team;
- To take action to rectify inaccurate data or complete incomplete information;
- To block, erase, or destroy inaccurate data;
- To prevent processing likely to cause damage or distress or for purposes of direct marketing;
- To object to any automated profiling without consent;
- To be provided their data in a structured, commonly used and machine-readable format and to have that data transmitted to another controller;
- Not to have significant decisions that will affect them taken solely by an automated process and to be informed of the mechanics of the automated decision-taking process that will significantly affect them;
- To request the relevant regulator to assess whether any provision of the Data Protection Legislation has been contravened; and
- To seek compensation if they suffer damage by any contravention of the Data Protection Legislation.

Complaints

A Data Subject has the right to complain at any time if they have concerns about how their information is used. If they wish to lodge a complaint against the Company, they can do so;

- By email to the legal.support@focusedgroup.co.uk;
- via our Data Protection Complaint Form, which can be provided upon request;
- via our online complaint form; <https://focusedumbrella.co.uk/data-protection-complaint-form/>
- by post (c/o Privacy Team, PayStream Accounting Services Limited, Mansion House, Manchester Road, Altrincham, WA14 4RW);
- verbally (including by telephone); or
- through any other reasonable communication channel we provide.

A Data Subject also has the option to complain directly to the Information Commissioner's Office via their website if they believe there has been a contravention of the UK GDPR. The ICO recommends individuals raise their concerns with the organisation first before approaching the ICO.

Further information can be found in our Data Protection Complaints Policy.