



Focus Consultants: Data Protection Policy

Introduction

This policy is to be used in conjunction with the Privacy Statements designed to form part of this policy as appendices, plus our Data Retention Policy.

We have a duty to notify you of the information contained in this policy.

Overview

Focus Consultants takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the UK General Data Protection Regulations (UK GDPR) in respect of data privacy and security. We are cognizant of the rolling changes being introduced by the Data Use and Access Act 2025 (DUAA) modifying the application of the existing legislation.

This policy applies to current and former employees, clients / project contacts, workers, volunteers, apprentices and consultants. If you fall into one of these categories you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment / services and any other notice we issue from time to time in relation to your data.

The Company is a 'data controller' for the purposes of certain employee, client and working partner personal data. This means that we determine the purpose and means of the processing of your personal data. Where we have your personal data on file but do not determine the purpose and means of the processing we act as 'data processor' only. This applies when we are provided with your details by, for example, our client who determines the manner in which we may use that data to allow us to discharge our duties.

This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

This policy does not form part of any contract of employment (or services if relevant) and can be amended by us at any time. It is intended to comply with the 2018 Act and the UK GDPR plus DUAA amendments. If any conflict arises between any other laws and this policy, the 2018 Act and the UK GDPR prevail.

Impact

We set annual SMART objectives and plan our corporate responsibility initiatives by targeting actions under the banners of Environment, Society and Governance and logging these centrally. Focus strives to advance our contributions to the UN Sustainability Development Goals through all company policies and activities.

This policy is designed to primarily contribute to the following goals:



In implementing this policy, Focus Consultants targets UN Sustainable Development Goals 9&16

Data Protection Principles

Personal data must be processed in accordance with the 'Data Protection Principles', which demonstrate:

- Fair, lawful, and transparent processing
- Purpose limitation
- Data minimisation
- Accuracy
- Data retention periods: 'storage limitation'
- Data security: 'integrity and confidentiality'
- Accountability.

We are accountable for these principles and must be able to show that we are compliant.

How We Define Personal Data

'Personal data' means information that relates to a living person (a 'data subject') who can be identified from that data on its own, or when taken together with other information that is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymized/pseudonymised data where the subject cannot be identified.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

We may collect and use the following types of personal data, where relevant:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your sex/gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving license and information in relation to your immigration status and Right to Work in the UK;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;

- training records;
- electronic information in relation to your use of IT systems/telephone systems;
- your images (whether captured on CCTV, by photograph or video);
- any other category of personal data, of which we may notify you from time to time.

We will only capture that data necessary for the purpose intended and will only hold data for as long as necessary.

How We Define Special Categories of Personal Data

'Special categories of personal data' relate to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sexual orientation; and
- any criminal convictions and offences.

We may hold and use any special categories of your personal data in accordance with the law, where relevant.

How We Define Processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data that forms part of a filing system and any automated processing.

How Will We Process Your Personal Data?

The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can usually only do this if your interests and rights do not override ours (or theirs). This is not the case for 'recognised legitimate interests' per Appendix 1 You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in the sections below.
- Under DUAA, we are also now permitted to process your data for purposes of protecting national / public security and defence; responding to an emergency; investigating crime; and safeguarding.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details, we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties, such as paying the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

Examples of When We Might Process Your Personal Data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example (and see below for the meaning of the asterisks):

- to decide whether to employ (or engage) you.
- to decide how much to pay you, and the other terms of your contract with us.
- to check you have the legal right to work for us.
- to carry out the contract between us including where relevant, its termination.
- training you and reviewing your performance*.
- to decide whether to promote you.
- to decide whether and how to manage your performance, absence or conduct*.
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else.
- to determine any reasonable adjustments required to your workplace or role because of your disability*.
- to monitor diversity and equal opportunities*.
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers, and others.
- to monitor and protect the health and safety of you, our other staff, customers and third parties*.
- to pay you and provide pension and other benefits in accordance with the contract between us*.
- paying tax and national insurance.
- to provide a reference upon request from another employer or similar (e.g. property agent).
- to pay trade union subscriptions*.
- monitoring compliance by you, us and others with our policies and our contractual obligations*
- to comply with employment-, immigration-, health and safety-, taxation- and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future.
- the prevention and detection of fraud or other criminal offences.
- to defend Focus in any investigation or litigation and to comply with any court or tribunal orders for disclosure*
- for any other reason, of which we may notify you from time to time.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data, then we would explain the reasons for our request. You do not need to consent and can withdraw your consent later if you choose by contacting our administration team.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes:

- where it is necessary for carrying out rights and obligations under employment law.

- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent.
- where you have made the data public.
- where processing is necessary for the establishment, exercise, or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

For recruitment purposes, we may request information surrounding criminal convictions. This will happen when you have applied for a position to work with us and have been shortlisted for selection after a successful interview. This is necessary because some of the duties you perform for us may require mandatory DBS checks, as some of our sites will put our staff in contact with vulnerable individuals or minors.

Certain checks may also be relevant for applications to a financial position within Focus to be subject to checks for previous convictions related to a charge of fraud or similar. This might be necessary to protect the company assets and those of our customers. Only details of those convictions relevant to the position will be retained and processed and will be subject to our most rigorous security procedures and treated as highly sensitive.

We only request such data if we satisfy Articles 6, 10 & the conditions in Principles 1, 2, 3, of Schedule 1, DPA 18.

We might process special categories of your personal data for the purposes in paragraph above which have an asterisk * beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation, or sex/gender to monitor equal opportunities.
- your sickness absence, health, and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety.

We do not take automated decisions about you using your personal data or use profiling in relation to you. For optimal security, our company policy is to handle all data other than name, address, email and telephone number as if it were special category information, labelling it clearly if sensitive or restricted and securing it appropriately.

Sharing Your Personal Data

Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send your personal data outside the EEA. If this changes you will be notified of this and the protections in place for the security of your data will be explained. We will share the minimum required information with UK based third parties, to allow us/them to fulfil contractual obligations or to secure benefits and funding to support your role or training. You should tell us if we may not share your details with other parties in this manner.

How Should You Process Personal Data for The Company?

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Retention policy.

The Company's Operations Manager, Sonja Greenhow, is our main contact in respect of Data Protection and will ensure this policy is reviewed and the Partners updated on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of, the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should keep personal data secure and not share it with unauthorised people or share personal data informally.

You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change so that we can maintain accurate records.

You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

You should use strong passwords and lock your computer screens when not at your desk.

Personal data should be encrypted or sent by other secure means when being transferred electronically to authorised external contacts. [Speak to IT for more information on how to do this.]

Anonymise /pseudonymise data or use separate keys/codes so that the data subject cannot be identified.

Do not save personal data to your own personal computers or other devices.

Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Partners.

You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

You should not take physical personal data away from company's premises without authorisation from your line manager/ a Partner and be particularly mindful of processing and privacy requirements when working remotely.

Personal data hard copies should be shredded and disposed of securely when you have finished with them.

You should ask for help from our Operations Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request. This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

How to Deal with Data Breaches

We have robust measures in place to help prevent data breaches. Should a breach of personal data occur (whether in respect of you or someone else) we must keep evidence of that breach.

If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the Operations Manager immediately and keep any evidence in relation to the breach.

Subject Access Requests

Data subjects can make a 'data subject access request' ('DSAR') to find out the information we hold about them. This request must be made in writing. You should forward such requests immediately to the Operations Manager who will coordinate the response.

If you would like to make a DSAR in relation to your own personal data you should write to the Operations Manager, our central Data Protection contact. We must respond within one month unless the data requested is complex or numerous, in which case the period in which we must respond can be extended by a further two months. You will be informed within the first month if this extension applies to your request.

The DUAA introduces a 'stop the clock' provision where additional evidence is requested from the complainant. The timeline restarts once further information is received.

There is no fee for making a DSAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request. We are required only to make 'reasonable and proportionate' searches to make this response, but firms must explain when they withhold data due to legal professional privilege / client confidentiality. You will be informed of the reason for applying this exemption.

Your Data Subject Rights

You have the right to information about what personal data we process, how and on what basis as set out in this policy.

You have the right to access your own personal data via a subject access request (see above).

You can correct any inaccuracies in your personal data. To do so, you should contact the Operations Manager.

You have the right to request that we erase your personal data where we were not entitled under the law to process it, or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the Operations Manager.

When requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Operations Manager.

You have the right to object to data processing where we are relying on a legitimate interest to do so, and you think that your rights and interests outweigh our own and you wish us to stop.

You have the right to object if we process your personal data for the purposes of direct marketing.

You have the right to receive a copy of your personal data and to transfer it to another data controller. We will not charge for this and will in most cases aim to do this within one month.

With some exceptions, you have the right not to be subjected to automated decision-making. Please note we do not use this method of decision making at present.

You have the right to be notified of a data security breach concerning your personal data.

In most situations we will not rely on your consent as lawful grounds to process your data. If we do, however, request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Operations Manager.

Complaints

Under the Data Use and Access Act 2025 (DUAA), organisations in the UK are legally required to implement a formal process for handling data protection complaints. A complaint may be any expression of dissatisfaction about how personal data is processed (e.g. collected, stored, shared). This includes concerns about subject access requests or other data rights. Under the new rules, you must approach the company first regarding complaint resolutions, prior to ICO contact.

We offer a range of contact methods (per Section 164A of the DPA 2018 as amended). Complaints may be made via email submission, by post to our Head Office address, or (initially) via our reception on 0115 9765050. See also our contact section of our website <https://www.focus-consultants.com/contact/>.

We usually ask you to supplement a telephone call with a written account to ensure consistency in data captured (e.g. name, contact details, description of complaint specifics, supporting evidence) plus check your identity prior to investigating, especially for sensitive matters.

Your complaint will be acknowledged within 30 calendar days and inquiries will be started promptly, aiming to conclude within a reasonable timeframe. You will be kept informed of progress including any delays.

We will communicate the outcome clearly via a written decision (email by default). This will include findings, any remedial actions, and information on further rights (e.g. internal review or escalation to the ICO). Any internal review will be undertaken by another staff member within a further 30 days unless otherwise agreed.

You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk) and in our appended Privacy Statement. This website has further information on your rights and our obligations.

Related Policies and Documentation:

Data Retention Policy
IT/ICT Policy
Cyber Security Policy
Home Working Policy
Disciplinary Policy
Privacy Statements

Monitoring

The effectiveness of this policy will be regularly reviewed by the Partners. Audits will occur at least annually in line with ISO 9001 practices.



For Focus Consultants 2010 LLP
Jason Redfearn BSc (Hons) MRICS
Partner
January 2026

Previous Issues

Date	Amendment	Reviewer
24.04.2018	Added references to GDPR, 2018 DPA (from 1998)	S Greenhow
06.11.2018	New format, new contact name added	S Greenhow
21.01.2021	Minor wording update for clarity, typo correction	S Greenhow
28.01.2022	Refresh Branding, new signatory	S Greenhow
21.01.2023	Minor update - typo correction; UK GDPR specifically referenced	S Greenhow
30.01.2024	Section updates to add related policies and monitoring	S Greenhow
05.02.2025	Refresh Branding, format. References contact title, clearer links with Privacy Policies – removed repetition.	S Greenhow
15.07.2025	Updated with amendment following DUAA introduction.	S Greenhow
08.01.2026	Minor wording update	S Greenhow