

# Privacy Policy

---

## **Purpose and scope**

Copper Consultancy (“Copper”, “we”, “us”, or “our”) is committed to protecting and respecting the personal data that we hold in accordance with the Data Protection Act 2018 (Act). This policy gives detailed guidance on how and why Copper processes and stores personal data held by the Company, and explains your rights to access the information we hold about you.

Personal data is any information relating to an identified or identifiable living person.

This policy applies to personal data that is provided to us either directly from the individual concerned, from a third party acting on behalf of an individual, from clients and their authorised agents, or from publicly available sources (such as internet searches, Companies House, etc.). Where we receive personal data that relates to an individual from a third party, we request that this third party informs the individual of the necessary information regarding the use of their data. Where necessary, reference may be made to this Privacy Policy.

We may use personal data provided to us for the purposes described in this Privacy Policy or as made clear before collecting personal data.

## **Processing data**

The Company will process all data in accordance with the GDPR’s Six Principles and the principles of the Act.

Personal data must:

- be processed fairly, lawfully and in a transparent manner;
- be obtained only for specified, explicit and lawful purposes and shall not be processed in any manner incompatible with those purposes;
- be adequate, relevant and limited to what is necessary to fulfil those purposes;
- be accurate and kept up to date;
- not be kept for longer than is necessary to fulfil those purposes;
- be processed in accordance with the rights of individuals under GDPR and the Act;
- be kept safe from unauthorised access, accidental loss or destruction; and
- not be transferred to a country outside the European Economic Area, unless that country has adequate levels of protection for personal data.

Where personal information is collected, the Company will ensure that:

- the purpose for which it is being collected is clear and information required to process it fairly is explained;
- the individual has given consent to the processing of information (unless the Company is otherwise satisfied it is processing the information lawfully);
- data is retained only for the length of time required for the purpose it was collected and compliance checks are carried out;
- appropriate technical and organisational security measures to safeguard personal information are applied.

In addition, the Company will ensure that:

- there is someone with specific responsibility for data protection throughout the Company;
- everyone managing and handling personal information is appropriately trained and understands that they are responsible for adhering to good data practice;
- queries about handling personal information are promptly and courteously dealt with;
- a regular review and audit is made of the way personal information is managed;
- methods of handling personal data are regularly assessed and evaluated.

## Lawful Processing

The lawful bases for processing stipulates that at least one of these must apply whenever personal data is to be processed:

- (a) Consent: you have given Copper (*e.g. any of the following depending on the situation freely, specific, informed or unambiguous*) consent for your personal data to be processed for a specific purpose.
- (b) Contract performance: the processing is necessary for the performance of a contract you have with Copper, which had asked you to take specific steps before entering into a contract.
- (c) Compliance with legal obligation: the processing is necessary for Copper to comply with the law (*e.g. the tax/social security obligation/employment law*) (*not including contractual obligations*).
- (d) Protection of vital interests: the processing is vital to an individual's survival.
- (e) Public interest: the processing is necessary for Copper to perform a task that is in the public interest or for its official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests: the processing is necessary for Copper legitimate interests, or the legitimate interests of a third-party, unless there is a good

reason to protect the individual's personal data that overrides those legitimate interests.

## What personal data do we hold and why

The personal data that is processed is dependent on specific client and project requirements, the business services we provide and receive, employment and recruitment requirements.

### Client personal data

It may be necessary for us to collect relevant financial or non-financial information to provide our services to government, businesses, not-for-profit and other organisations. As an example, this may include contact details, employee information, lists of shareholders, customers and suppliers and any other specifically relevant data.

Client data is collected for professional services, and is used for the following purposes:

- **Client management** - when communicating with and assessing the needs of clients, personal data may be processed in order to ensure that their needs are appropriately satisfied;
- **Administration** - in order to manage and administer our business and services, we may collect and process personal data. This may include (but is not limited to) maintaining internal business records, managing client relationships, hosting events, administering client facing documents, and maintaining internal operating processes;
- **Regulatory** - in order to undertake professional services, we may from time to time be required to collect and process personal data to fulfil regulatory, legal or ethical requirements. This may include (but is not limited to) the verification of identity of individuals.

### Project-related personal data

Personal data may include name, address, email, phone number; records of correspondence via phone, email, post; and any other relevant information regarding stakeholders and members of the public. This information may be obtained (but is not limited to) internet searches, Royal Mail data, the electoral roll, public events, feedback forms, email, website, phone conversations, door to door visits or other public records, or from clients and their authorised agents in fulfilling the needs and purpose of the project.

Project-related data is used for, but not limited to:

- stakeholder mapping;
- stakeholder and public consultation and engagement;
- registering for project-related updates;
- recording attendance at exhibitions and other events;
- stakeholder relationship management;
- collation of feedback, and evidence of consultation/engagement;



- media management.

### Supplier and sub-contractor data

Personal data may include contact names, contact details, identity documents and details, insurance details and relevant policies and procedures. We share data with suppliers and sub-contractors (including, for example, sub-contractors providing payment and delivery services, and credit reference agencies).

Supplier and subcontractor data is held to:

- manage our business relationships;
- contract and receive services from them;
- and in some cases to provide professional services to clients.

### Business contacts

Personal data from our contacts, including potential and former clients, are held in our customer relationship management system (CRM system), financial software and secure server files. This information is entered into these systems after contact is made between a staff member of Copper Consultancy and an individual business contact. This information may include name, contact details, work history, profiles, details of correspondence and other communication.

Personal data held on business contacts is used for the following purposes:

- promoting and developing our services and products;
- communication of technical updates;
- hosting and facilitating events;
- relationship management;
- administration and management.

We may use business contact details to provide information that we think will be of interest about us and our services: for example, industry updates and insights; Copper's newsletter; other services that may be relevant and invites to events. Personal information that is out of date and where contacts request that they no longer wish us to send them updates is deleted.

### Employees, former employees and associates

The Company needs to collect and use certain types of information about employees in order to operate the business and to fulfil its legal obligations.

Employee personal data may include name, address, personal email, phone number, date of birth, gender, nationality, work history, employment records, national insurance number, bank account and other financial records, passport information, driving licences and other documents used for ID purposes, details of next of kin and emergency contacts, references and other relevant work-related information for as long as is required by law



or deemed necessary by the Company for the purpose of fulfilling its employment obligations.

Consent to process personal and sensitive data is sought when a new employee signs an employment contract or during an induction programme.

Personal data held on employees, former employees and associates is used for, but is not exclusive to, the following purposes:

- Legislative employment requirements;
- Personnel management requirements;
- Employment administration and payroll;
- References.

All information containing personal data is carefully classified and protected against unauthorised access, accidental loss or destruction, modification or disclosure.

Further information about how the Company handles personal data for employment purposes is contained in a separate data protection policy for employees.

### Job applicants

We process personal data relating to those who respond to job vacancies or who send us speculative job applications. We do this for employment purposes, to assist us in the selection of candidates for employment, and to assist in the running of the business. Personal data may include identifiers such as name, date of birth, personal characteristics such as gender, nationality, qualifications and previous employment history.

We will not share any identifiable personal data with third parties without consent unless the law allows or requires us to do so. Personal data provided during an application process will be retained for a period of six months in case a further vacancy arises or, if required by law, for as long as is required.

This privacy notice does not form part of an employment offer or contract between Copper and a prospective employee. If we make an employment offer, we provide further information about how we handle personal data for employment purposes separately.

### People who use our website and social media

When people visit our website, personal data is collected both through automated tracking and by interacting in various forms on the website or social media (collectively referred to as websites). We also share data with third parties (including, for example, business partners, sub-contractors providing technical services, analytics providers and search information providers).

Personal data may be collected when individuals fill in forms on our websites or by corresponding with us by phone, email, social media or otherwise. This includes information provided when an individual makes contact with us via our websites, makes an enquiry, posts on social media, comments on blogs, subscribes to Copper's newsletter, responds to a survey, applies to work for Copper Consultancy or reports a problem with our websites.

Often, individuals who visit our websites additionally fall into another category as listed by this Privacy Policy. For instance, users of our websites may be current clients, business contacts or become clients in the future. Where this is the case, personal data held and processed about individuals who use our website may also become personal data that is held and processed for another purpose.

There are several reasons why we will process personal data that an individual may provide to us when visiting our websites. These include;

- **Administration** - to administer our site and improve internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes. For example, we use this data to ensure that the website is presented well for individuals and is optimised appropriately;
- **Functionality** - to allow individuals to use some functionality of our websites, certain personal data must be entered in order for features to work as intended;
- **Security** - to keep our websites safe and secure, we may sometimes collect personal data, such as login information and other data that can be used to vouch an individual's identity;
- **Promotion and development of our services and products** - some personal data may be used to measure or understand the effectiveness of promotion to individuals.

The personal data we hold depends on what data was entered and for what purpose. Where data was entered to engage with functionality of our websites, that personal data may include an individual's name, address, email address and phone number.

Where personal data is collected automatically, the data that we may collect includes technical information, including the internet protocol (IP) address used to connect an individual's computer to the internet, login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform. Other technical data about an individual's visit will also be collected, including the full Uniform Resource Locators (URL) clickstream to, through and from our websites (including date and time); products viewed or searched for; page response times; download errors; length of visits to certain pages; page interaction information (such as scrolling, clicks, and mouse-overs); and methods used to browse away from the page and any phone number used to call our customer service number.



Our websites use cookies to distinguish individuals from one another. This helps us to provide a better experience when individuals browse our websites and also allows us to improve our websites. For detailed information on the cookies we use and the purposes for which we use them, see our Cookie Policy.

## Location of processing

Where possible, personal data resides within the UK but may be transferred to, and stored at, a destination outside the European Economic Area (EEA). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. We will take all reasonable steps to ensure that personal data is treated securely, in accordance with this Privacy Policy.

We have taken steps to ensure all personal data is provided with adequate protection and that all transfers of personal data outside the EU are done lawfully. Where we transfer personal data outside of the EU to a country not determined by the European Commission as providing an adequate level of protection for personal data, the transfers will be under an agreement which covers the EU requirements for the transfer of personal data outside the EU.

## Data security

We take the security of all the data we hold seriously. Staff are trained on data protection, confidentiality and security. Copper takes reasonable precautions at all times to guard data against any unauthorised access and use. Appropriate technical and organisational measures are taken to prevent the unauthorised or unlawful processing and accidental loss or damage of personal data.

These provisions also apply to data kept on open access within Copper (such as contact files and databases) and data taken off Company premises (such as personal data kept in laptops, mobile telephones and in computers used for work purposes at home).

We have a framework of policies and procedures which ensure we regularly review the appropriateness of the measures we have in place to keep the data we hold secure.

All Copper IT systems are configured to enforce the following:

- Authentication of individual users;
- Protection with regards to the retrieval of passwords and security details;
- System access monitoring and logging – at a user level;
- Access to the network connection is secured by two factor authentications consisting of a username and one other component.

We have security measures in place to protect our and our clients' information (including personal data), which involve detecting, investigating and resolving security threats. Personal data may be processed as part of the security monitoring that we undertake; for

example, automated scans to identify harmful emails. We have policies and procedures in place to monitor the quality of our services and manage risks in relation to our suppliers. We collect and hold personal data as part of our supplier contracting procedures. We monitor the services provided for quality purposes, which may involve processing personal data.

## Sharing data

We will only share personal data with others when we are legally permitted to do so. When we share data with others, we put contractual arrangements and security mechanisms in place to protect the data and to comply with our data protection, confidentiality and security standards.

Personal data held by us may be transferred to:

- Clients and their authorised agents to fulfil their legitimate interests and legal obligations;
- Third party organisations that provide applications/functionality, data processing or IT services to us;
- Third parties that support us in providing our services and to help provide, run and manage our internal IT systems. For example, service providers of information technology, cloud based software, identity management, website hosting and management, data analysis, data back-up, security and storage services. The servers powering and facilitating that cloud infrastructure are located in secure data centres around the world, and personal data may be stored in any one of them;
- Third party organisations that otherwise assist us in providing goods, services or information;
- Auditors and other professional advisers;
- Law enforcement or regulatory agencies or third parties as required by law or regulations.

Occasionally, we may receive requests from third parties with authority to obtain disclosure of personal data, such as to check that we are complying with applicable law and regulation, to investigate an alleged crime, to establish, exercise or defend legal rights. We will only fulfil requests for personal data where we are permitted to do so in accordance with applicable law or regulation.

## Data retention and destruction

All personal data, whether in paper or electronic form, will be retained in line with our RR&D Policy and destroyed or erased securely to avoid any risk of unauthorised access or use once this data is no longer in use.

## Training



Copper is committed to ensuring all employees who are responsible for compliance with the Act, can exhibit competency in their understanding of the Act, and are implementing good practice in their day-to-day work.

All persons with responsibility for the Act receive appropriate training and all training records are maintained by Copper's HR department.

Copper ensures that all persons responsible for compliance with the Act are regularly informed of and updated on all relevant matters related to personal data management, including through contact with external bodies, the most noteworthy of which is the Information Commissioner's Office (ICO) - [www.ico.gov.uk](http://www.ico.gov.uk).

## Individuals' rights

Copper recognises that individuals have certain rights over their personal data and where the Company is a data controller, it has responsibility for fulfilling these rights as follows:

- Individuals may request access to their personal data held by Copper as a data controller;
- Individuals may request Copper to rectify personal data submitted to the Company or, where appropriate, contact Copper via the relevant website registration page or by amending the personal details held on relevant applications with which they registered;
- Individuals may request that Copper erases their personal data;
- Where Copper processes personal data based on consent, individuals may withdraw their consent at any time by contacting the Company or clicking on the unsubscribe link in an email received from Copper;
- Individuals may have other rights to restrict or object to Copper's processing of personal data and the right to data portability;
- Individuals may request information about, or human intervention into, any automated data processing that Copper may undertake.

If individuals wish to exercise any of these rights, they are requested to send an email to [info@copperconsultancy.com](mailto:info@copperconsultancy.com).

## Contact information and complaints

If an individual has questions about this Privacy Policy, how and why Copper processes personal data or wishes to make a complaint, they may contact the Head of Data Privacy at [info@copperconsultancy.com](mailto:info@copperconsultancy.com) or by post to Copper Consultancy, 120 Regent Street, London, W1B 5FE.

Copper will look into and respond to any complaints received.



Copper also recognises that an individual has the right to lodge a complaint with the UK data protection regulator, ICO. For further information on individuals' rights and how to complain to ICO, please refer to the ICO website <https://ico.org.uk/concerns>.

Contact details:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Tel: 0303 123 1113 (local rate)

**Last updated: November 2021    Next review: November 2022**