



# Privacy Policy

---

## Who are we?

Copper Consultancy is a company registered in England and Wales (number 03030759). Our registered address is 120 Regent Street, London, United Kingdom, W1B 5FE.

References in this Privacy Policy to 'Copper', 'we', 'us' or 'our' mean 'Copper Consultancy'.

We specialise in the development of economic and social infrastructure and in so doing, we work with some of the largest organisations in the UK, and on some of the most contentious projects, helping to explain their benefits, build understanding and create advocacy.

Detailed information about our company and our services can be found on our website: <https://www.copperconsultancy.com>

## Who is responsible for your data?

Copper Consultancy is a 'data controller' for the purposes of the Data Protection Act 2018 ('Act') and the UK General Data Protection Regulation ('UK GDPR'): we are registered with the Information Commissioner's Office (ICO), registration number Z8724811.

Copper is committed to respecting and protecting your privacy. Please read this Privacy Policy carefully to understand our practices regarding the processing your personal data.

Our Head of Data Privacy can be contacted via: [info@copperconsultancy.com](mailto:info@copperconsultancy.com)

## Purpose and scope

The UK GDPR defines 'personal data' as any information relating to an identified or identifiable living person (sometimes referred to as a 'natural person' or 'data subject').

This Privacy Policy sets out the lawful basis for processing the personal data that we collect from you, or that you provide to us, and explains our purpose for doing so. It also explains your data subject rights, for instance, your right to access the information we hold about you, and it explains how you can exercise your rights.



This Privacy Policy applies to personal data that is provided to us either directly from you, from a third party acting on your behalf, 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 the 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 the personal data provided to us for the purposes described in this Privacy Policy or for purposes that are made clear at the point of collecting the personal data.

## Processing data

The data processing principles contained in the UK GDPR require personal data to be:

- processed fairly, lawfully and in a transparent manner;
- obtained only for specified, explicit and lawful purposes and shall not be processed in any manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary to fulfil those purposes;
- accurate and kept up to date;
- not be kept for longer than is necessary to fulfil those purposes; and
- kept safe from unauthorised access, accidental loss or destruction;

Additionally, personal data collected by us will be:

- processed in accordance with the rights of data subjects;
- not be transferred to a country outside the European Economic Area (EEA), unless that country has adequate levels of protection for personal data.

Where personal information is collected, we will ensure that:

- the purpose for which it is being collected is clear and explain our processing activities in a fair and transparent manner;
- we have a lawful basis for processing someone's personal data e.g. their consent;
- data is retained only for the length of time required for the purpose it was collected and that checks are carried out by us to ensure that data is being deleted;
- appropriate technical and organisational security measures are applied to safeguard the personal data that we are processing.



In addition, we will ensure that:

- a senior member of our company has specific responsibility for data protection;
- everyone managing and handling personal information is appropriately trained and understands that they are responsible for adhering to the law/best practice;
- queries about handling personal information are promptly and courteously dealt with;
- regular reviews and audits of our processing activities are conducted;
- methods of handling personal data are regularly assessed and evaluated.

## Lawful Processing

The lawful bases for processing are set out in Article 6 of the GDPR. 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 depends 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), 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; and
- 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, or where contacts request us to stop sending them updates, is deleted.

### Employees, former employees and associates

We need to collect and use certain types of information about employees in order to operate the business and to fulfil our 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 licenses 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 us 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 Copper handles personal data for employment purposes is contained in a separate 'Staff Privacy Policy'.

### 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.

### 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 share this 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 collected from people who visit 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. When this occurs, we will take all reasonable steps to ensure that personal data is processed securely, and 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 EEA are lawfully carried out.

Where we transfer personal data outside of the EEA, to a country not determined by the European Commission as providing an adequate level of protection for personal data, the transfers will only be undertaken in accordance with an agreement which covers the requirements of the UK GDPR for the transfer of personal data outside the EEA.

## 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 our premises (such as personal data kept on laptops, mobile telephones and in computers used for work purposes).

We regularly review the appropriateness of the measures we have in place to keep the data we hold secure.

Security measures are applied to Copper IT systems to protect ours and our clients' information (incl. personal data). These measures include:

- 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.

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 risk.



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 the disclosure of personal data where we are permitted to do so, in accordance with an applicable law or regulation.

## Data retention and destruction

All personal data, whether in paper or electronic form, will be retained in line with our Record retention & Disposal (RR&D) Policy RR&D Schedule. Personal data will be securely destroyed or erased to avoid any risk of unauthorised access or use of the data.



## Training

Copper is committed to ensuring that our employees can exhibit competency in their understanding of their data protection and privacy responsibilities, and that best practice is followed in their day-to-day work.

Staff with specific data protection and privacy responsibility receive appropriate training. Individual training records are maintained by Copper's HR department.

We ensure that all persons responsible for compliance with the Act are regularly updated on matters relating 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)

## What are my data subject rights?

We support the rights of data subjects as defined in Act and the UK GDPR, including:

- right to be informed (chiefly via this policy)
- right of access
- right to rectification
- right to erasure
- right to restrict processing
- right to data portability
- right to object
- rights related to automated decision-making including profiling

You can exercise your rights by contacting us using any of the methods shown below in the 'How do I contact you?' section. We will respond to your request as quickly as possible. Usually, this will be within one month of receiving your request.

## Updating my information

You may choose to correct, update, or delete your personal data, by contacting us using any of the methods shown below in the 'How do I contact you?' section.

If you have opted-in to receiving communications from us, your preferences will remain in effect until you tell us that you want to opt-out of receiving any further communications. Normally, you can do this by clicking the link at the footer of the email that we have sent to you.

You can change your preferences at any time by clicking the relevant link in the emails we send you or by contacting using any of the methods shown below in the 'How do I contact you?' section.



## Withdrawing my consent

Where we process your information based on your consent, you may withdraw your consent at any time. You can do this by contacting us using any of the methods shown below in the 'How do I contact you?' section.

## How do I contact you?

Should you wish to exercise any of your data subject rights, withdraw your consent to processing, complain about our use of your personal data, or report a personal data breach, you may do so using any of the methods shown below:

By post: Head of Data Privacy  
Copper Consultancy  
49 Carnaby Street  
London  
W1F 9PY

By email: [info@copperconsultancy.com](mailto:info@copperconsultancy.com)

We will deal with your enquiry as quickly as possible and respond appropriately.

## Making a complaint to the Information Commissioner

You can lodge a complaint with the Information Commissioner at any time. For instance, if you are unhappy with the way in which we are processing your information, or we have failed to facilitate your data subject rights.

For further information on individuals' rights and how to complain to ICO, please refer to the ICO website: <https://ico.org.uk/make-a-complaint/>

Alternatively, the ICO can be contacted as follows:

By post: Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

By phone: 0303 123 1113 (local rate)

## Review

We continuously review the content of our Privacy Policy to ensure it accurately reflects what we do with your information.



This Privacy Policy was last updated in November 2021.