



Policy and Processes	
Author	Steve Clarke
Policy / Process	Data Protection
Version/Date	V7.0 May '26

This Data Protection policy is aimed at making it possible for candidates and others who come in to contact with Tech Leaders Connect to understand how we use and protect personal data. Personal data is any data that can identify someone either on its own or if combined with other data.

Tech Leaders Connect is a provider of Fractional CIOs, but also has created a CIO/CTO Standard that enables CIOs/CTOs to demonstrate their capabilities to a wider world through independent assessment and certification.

We take the aspect of protecting personal data very seriously and are committed to protecting personal data by complying with relevant privacy legislation.

Legal Basis

We are required by law to always have a permitted reason called “lawful basis” for processing your personal data. There are six ways to process your personal data:

- Consent: Consent has been sought and provided for us to process your personal data
- Contract: Personal data is required for the delivery of a contract
- Legal Obligation: To comply with a legal obligation
- Vital Interests: To protect vital interests
- Public Task: To enable a task to be carried out in the public interest
- Legitimate Interest: Needed for the purpose of the legitimate interests

Data Processing

We may process the following types of data:

- Personal Data: Information that can be used to identify an individual, either directly on its own or in combination with other information such as a name, ID number, location data or an online identifier
- Pseudonymised: Personal data that can no longer be attributed to an individual without the use of additional information.
- Anonymised: Data in a form that does not identify individuals.
- Aggregated: Statistical data about multiple individuals combined to show trends, etc without identifying individuals within the data

We may collect, use, store or transfer different kinds of data that are grouped into the following categories:

- Identity Data includes first name, maiden name, last name, username or similar identifier, marital status, title and date of birth;
- Contact Data includes billing address, delivery address, email address and telephone numbers;
- Financial Data includes bank account and payment card details;
- Transaction Data includes details about payments to and from you and other details of products and services you have purchased from us;
- Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our websites;
- Profile Data includes your username and password, your interests, preferences, feedback and survey responses;
- Usage Data includes information about how you use our website, products and services, engage and interact with our systems;
- Marketing and Communications Data includes your preferences in receiving information and marketing from us and our third parties and your communication preferences;

We collect personal data in the following ways:

When personal data is requested, it will be made clear whether the personal data being asked for is required so that products and services can be made available to you or whether it is optional. We may use your personal data to fulfil a contract or take steps linked to a contract, for instance:

- Provide you access to membership benefits
- Provide you with information about your membership and your chosen products and services;
- To provide you with administrative support such as account creation, security and responding to issues;
- Fulfil payments for CIO/CTO Standard products and services;
- Provide you with newsletters, which include information about events, services or products that we may offer, that we feel may interest you or where you have consented to such communications;
- Carry out our obligations from any contracts you may have entered into with us;
- User/membership satisfaction surveys and market research;
- Respond to your enquiries and complaints;
- Notify you about changes to our terms of service;
- To provide an improved customer experience by recording calls and using them for training purposes
- Provide you with access to location, property and other appropriate data where you have agreed terms

Legitimate Interests

There are times when we will rely on Legitimate Interests to process personal data, particularly when it is not possible or practical to obtain consent. We will always consider if it is fair and balanced to use the data and if it is within reasonable expectations. We aim to balance an individual's rights with our legitimate interests to ensure that we use your personal information in ways that are not unduly intrusive or unfair, for example:

- Reporting criminal acts and compliance with law enforcement agencies;
- Internal and external audit for financial or regulatory compliance purposes;
- Statutory reporting;
- Performing analytics on sales or marketing data, determining the effectiveness of promotional campaigns;
- Operate our platforms and communicate with you as necessary when providing our services to you for our legitimate interest;
- Use analytics data collected when you consent to the use of Cookies and other tracking technologies;
- Improving the quality of experience when you interact with our products or services, including testing the performance and customer experience of our website;
- To enhance our offering, by identifying your interactions through our website, so that we can produce more relevant and engaging content;
- Physical and Network security;
- Financial Management and Control;

Device Information

Each time you visit our sites and/or our services, we may automatically collect information, including:

- Technical information, including the type of mobile device you use, a unique device identifier (for example, your Device's IMEI number, the MAC address of the Device's wireless network interface, or the mobile phone number used by the Device), mobile network information, your mobile operating system, the type of mobile browser you use, and/or time zone setting;
- Details of your visits to any of our Sites and Services including, but not limited to, Internet protocol (IP) address used by your Device, traffic data, weblogs and other communication data, whether this is required for our own billing purposes and/or the resources that you access (Log Information);
- URL click stream information showing how users have reached our Site and Services and whether they access other third-party sites via any external links

This information is used in the following ways:

- To administer our Sites and/or Services for troubleshooting, data analysis, testing, research, statistical and survey purposes;
- To improve our Sites and/or Services to ensure that content is presented in the most effective manner for you and for your Device;
- To allow you to participate in interactive features of our site or services, when you choose to do so;
- As part of our efforts to keep our Sites and/or Services safe and secure;
- To determine which features your Device supports which assists our development strategy

Sharing information with Third Parties

We may also share data with trusted third parties including:

- Service providers contracted to us in connection with the provision of products and services

- Regulators and related companies such as OfQual and SAIS
- Disciplinary Investigation panels and appeals panels
- Complainants
- Insurers
- Lawyers and/or specialist advisors

We also use payment providers to process payments and as such personal data will be provided to the relevant payment provider. We do not allow any third-party service provider to use personal data for their own purposes and only permit them to process personal data for specified purposes and in accordance to specific instructions.

Third Party Countries

Personal information may be transferred to, and processed in different countries in which a candidate is resident. Our systems are all based in the UK, but some of our service providers and partners operate in the UK, EEA or outside the EEA. This means that personal data may be processed in any of these countries. Safeguards are in place to ensure that personal data remains protected in accordance to this Privacy policy.

Storage of personal data

Personal data is stored as: secure physical records; electronically on our internal IT systems; in cloud storage, and in some cases, records on third party servers, which may be located in various countries.

Personal Data will be processed in a way that ensures appropriate security from unauthorised or unlawful processing, accidental loss, destruction or damage. Personal data is held in secure systems with controlled access and subject to cyber security measures, whether processed on site or working from home.

Third party service providers are chosen in line with company protocol, procedures and checks, and when they're used, we disclose only the personal information that is necessary to deliver the service provided.

There are procedures in place to deal with any suspected personal data breach and all of our employees must complete annual data protection training.

Personal Data Retention

Personal data is retained for as long as necessary to fulfil the purposes it was collected for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Personal Data may also be retained for a reasonable period afterwards to allow a response to any follow up enquiries or complaints, or for as long a candidate remains a registered user of our products and services.

Retention periods are worked out by considering the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of the personal data, the purposes for which it is being processed and whether the objective can be achieved through other means and the applicable legal requirements. In some circumstances personal data may be anonymised for research or statistical purposes and it then may be stored indefinitely without further notice.

In some circumstances data will be deleted on request: see Right to Erasure below for further information.

16. Data protection rights for UK and EEA Data Subjects

If you are a resident of the UK or EEA, you have the following data protection rights:

- Withdraw Consent - Where personal information based on your consent is being used, you have the right to withdraw that consent at any time.
- Right to be Informed – The right to be told how personal information will be used. This Privacy Policy document, is intended to be a clear and transparent description of how data may be used.
- Right of Access – The right to find out what information is held and to request a copy of that information. This is called a Subject Access Request. Subject Access Requests provide 30 days to respond once it is established there is a right to see the requested records and identity has been successfully confirmed.

Details on how to submit a Subject Access Request if you are in the UK or EEA can be found on our data protection page. Individuals cannot use a Subject Access Request to obtain examination papers, examination answers to questions, or scripts, as this is exempt under the Data Protection Act Schedule 2 Part 4 Clause 25.

- Right of Erasure –The right to be forgotten (i.e. to have personally identifiable data deleted). However, it may not always be able to comply with a request of erasure for specific legal reasons, which will be notified. In some cases, suppressing future communications may be the appropriate option rather than data deletion.
- Right of Rectification – If records are inaccurate there is the right to ask for those records to be updated. This enables any incomplete or inaccurate data held to be corrected. The accuracy of the new data provided may need to be verified.
- Right to Restrict Processing – In certain situations there is the right to ask for processing of personal data to be restricted because there is some disagreement about its accuracy or legitimate usage.
- Right to Data Portability – Where personal data is being processed under your consent, the law allows for data to be ported from Tech Leaders Connect to another service provider. This right is largely seen as a way for people to transfer personal data from one service provider to another. We will provide personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which has been provided consent for use or where the information is used to perform a contract.
- Right to Object - The right to stop the processing of personal data for direct marketing purposes. Simply contact Customer Service they will amend contact preferences
- Right to object to automated decisions – In a situation where a data controller is using personal data in a computerised model or algorithm to make decisions “that have a legal effect on you”, the right to object is available. This right is more applicable to mortgage or finance situations. No complex computerised decisions are made that produce legal effects.

Cookies

Cookies are used to distinguish individuals from other users of our Sites and Services. This helps to provide a good experience when using Sites and Services and allows for

improvements. Browsers can be set to refuse all or some browser cookies, or to alert when websites set or access cookies. Disabling or refusing cookies may result in some parts of the website becoming inaccessible or not

function properly. Detailed information on cookies used and the purposes they're used for can be found in the cookie policy here <Link>

Additional information for international users (outside of the UK or EEA)

If you are accessing our Sites and/or Services from outside the UK or EEA, you may have rights under your residing countries privacy laws.

Nothing in this Privacy Notice purports to exclude, modify or restrict your rights under those laws.

Any changes made to the Privacy Notice in the future will be posted on the website and, where appropriate, notified to individuals affected. The new terms may be displayed on-screen, and we may require them to be read and accept them to continue use of any Services.

Contact Us

To contact us about the use of personal data, or exercising personal rights, please contact us at:

Email: <Email> for any requests to stop processing your data

Email: <Email> for any Data Subject Access Requests

Phone: + 44 (0) 203 020 1864

Lines are open Monday to Friday, 08:30 to 17:15 BST (UK Time)

Your Right to Complain

If there is a view that data protection rights have been breached and there is a concern, everyone has the right to report those concern to the local data protection supervisory authority. In the UK this is the Information Commissioner's Office (ICO) and concerns can be raised by going to ICO website.