Privacy Policy [Last updated 1st August 2021.Headings updated 1st June 2023]

Who We Are

We are WorkInConfidence Limited, ("WIC") a company incorporated in England and Wales with registered address at Greyfriars Gate, Greyfriars Road, Reading, Berkshire, England, RG1 1NU and registration number 08255296

We are registered with the ICO as a fee payer with registration number Z3403582

Our Data Protection Officer can be contacted by emailing dpo@workinconfidence.com

We provide a system which makes it easier for staff to give feedback to their organisation in a tried and trusted way.

1. Users of Our Platform and Our Role

This is the Privacy Policy for Users of the WorkInConfidence Online Platform / Web App. Section 3 Below also applies to you.

We routinely act as a Joint Controller with your employer. Please note this is not always the arrangement. You can always contact your employer or WorkInConfidence (dpo@workinconfidence.com) if you would like further clarification.

Where we are Joint Controllers with your employer, we work together to allow access to the WIC platform for the purpose of giving employees an independent platform to voice workplace concerns and provide feedback and views IN A SAFE WAY WHERE YOUR IDENTITY IS PROTECTED (UNLESS YOU DECIDE AT ANY TIME TO SAY WHO YOU ARE).

WorkInConfidence specifically manages the registration process and the process of making sure the identity of people who voluntarily choose to register on the platform is not disclosed to their employer, where this represents the wishes of individuals. Unless people chose to self-identify, via the platform. Please also see our Individual Terms: https://www.workinconfidence.com/individual-terms/.

Your employer manages any personal data handled or collected for the following reasons; providing email address for registration purposes, assigning manager or admin status to specific employees, conducting surveys, running discussion boards, any case management conducted via the WIC platform, and any other circumstances in which you choose to self-identify. This does not affect our undertaking to protect your identity unless you decide or agree otherwise.

Where we are a Processor of personal data, we do so on the instruction of another organisation – probably your employer (the Controller). IF WE DO ACT AS PROCESSOR, WE STILL ENSURE THAT WE ARE IN A POSITION TO PROTECT YOUR IDENTITY (UNLESS YOU DECIDE AT ANY TIME TO SAY WHO YOU ARE).

For users or our platform we routinely process a work email address. For some people such as managers we may include name, job title, mobile phone number. You may also input certain other information and any personal details users provide via their use of the platform.

Your Rights

All individuals (users of our platform or otherwise) have a number of rights with regards to your personal data under the Data Protection Laws. If you wish to exercise any of your rights, please contact us at dpo@workinconfidence.com

- Right of access: You can request access to a copy of the personal data which we hold about you, as well as details about why and how we use it.;
- Right to rectification: You can ask us to change or complete any personal data we hold about you which is inaccurate or incomplete;
- Right to be forgotten/erasure: You have a right, under certain circumstances, to ask us to delete any personal data we hold about you. Please note that there may be situations where we must retain your personal data after a request for erasure where we have a lawful basis for doing so;
- Right of restriction: You can ask us to restrict (i.e. prevent) the processing of your personal data where you have objected to our use of it and we have no lawful basis to continue processing your personal data;
- Right of data portability: In certain circumstances, you can ask us to transfer the data we hold about you to another organisation. This would be sent in a structured, commonly used, electronic form;
- Right to object: You can object to us using your personal data for particular purposes; and
- Automated decision making: You have a right not to be subjected to automated decision making and profiling in certain situations.

If you have any cause to complain about our use of your personal data, please contact us by emailing dpo@workinconfidence.com

You also have the right to lodge a complaint about our processing with a supervisory authority — in the UK that is the ICO whose details are here: https://ico.org.uk/make-a-complaint/

Automated decision making

We do not use your personal data in any automated processes to make decisions about you

What Happens If Our Business Changes Hands?

We may, from time to time, expand or reduce our business and this may involve the sale and/or the transfer of control of all or part of Our business. Any personal data that you have provided will, where it is relevant to any part of our business that is being transferred, be transferred along with that part and the new owner or newly controlling party will, depending on the lawful basis, be permitted to use that data only for the same purposes for which it was originally collected by Us.

In the event that any of your data is to be transferred in such a manner, you will be contacted in advance and informed of the changes.

Changes to Our Privacy Policy

We may change this Privacy Policy from time to time (for example, if the law changes). We recommend that you check this page regularly to keep up-to-date.

If we make any material changes to the manner in which we process and use your personal data, we will contact you to let you know about the change.

Get in touch

If you have queries about our use of your data, please contact us by emailing us on dpo@workinconfidence.com

2. Other Individuals

In addition to the information provided above for users of our platform we also act as a Controller for the following type of individuals; WIC's employees, job applicants, suppliers, clients, prospects, investors and website visitors.

What Personal Data Does WIC Process?

You can find out more about the types of personal data we process for the above types of individuals here:

- I am a potential employee (see below section)
- I am a corporate client (see below section)
- I am a corporate prospect (see below section)
- I am a supplier to WIC (see below section)
- I am an investor/shareholder (see below section)
- I am just browsing your website (includes our cookie notice) (see below section)

Potential Employee Privacy Notice

Data that we hold and how we use it

As a potential employee we hold the following data on you:

Contact details, CV, and email correspondence with you. If you are successful in gaining employment with WIC then you will fall under the Employee Privacy Notice going forward.

Lawful basis for processing

Our lawful basis for processing your data is a combination of Contract, legitimate interest and consent. When you applied for a job it was with a view to entering into an employment contract with us. If we decide not to go forward with your application then we use legitimate interest to retain the data should the chosen candidate not work out or another role become immediately available.

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. We also transfer your data to our lawyers for contracting and to support with the visa sponsorship process if applicable. Where data is transferred outside of the EEA, we ensure that appropriate protection and mechanisms are in place, for example Standard Contractual Clauses. We do not sell your data to anybody.

Retention Periods

If you are unsuccessful in your application, we will keep your details on file for 3 months after the position is filled.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes.

Corporate Client Privacy Notice

Data that we hold and how we use it

As a corporate client, we hold the contact details required to carry out our contract with you, data to manage our relationship and keep you up to date with changes and improvements to our services. This data would have been sourced from you directly.

Lawful basis for processing

Our lawful basis for processing your data is a combination of Contract and Legitimate Interest. We use legitimate interest when we use your data to keep you up to date with changes and improvements to our goods and services. Our legitimate interest balancing test indicates that this is a legitimate purpose; it is necessary for the purpose of keeping you updated and growing our business, and unlikely to cause you risk or harm. All other data is processed to enable us to fulfil our contract with you and manage our relationship with you.

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. We also transfer your data to our accountants to ensure we are paid appropriately. Where data is transferred outside of the EEA, we ensure that appropriate protection and mechanisms are in place, for example, Standard Contractual Clauses. We do not sell your data to anybody

Retention Periods

We hold data on Corporate Clients for the length of time that you are a client of ours, then another 7 years in case of any dispute.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes.

Supplier Privacy Notice

Data that we hold and how we use it

As a supplier to WIC, we hold the contact and payment details required to carry out our contract with you and data to manage our relationship with you. This data would have been sourced from you directly, although your contact details may have been sourced from a recommendation or another source, with the intention of entering into a contact with you.

Lawful basis for processing

Our lawful basis for processing your data is contract; all data is used enable us to fulfil our contract with you, including paying you and managing our relationship with you.

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. We also transfer your data to our accountants to ensure you are paid appropriately. Where data is transferred outside of the EEA, we ensure that appropriate protection and

mechanisms are in place, for example Standard Contractual Clauses. We do not sell your data to anybody

Retention Periods

We hold data on suppliers for the duration of our contract, plus 7 years to account for accounting regulations and in case of any dispute.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes.

Prospective Client Privacy Notice

Data that we hold and how we use it

As a potential client, we hold your name, job title and corporate contact details so we can build a relationship with you. This data will have been sourced directly from you at an event, or from your company website or a similar publicly available source. We only hold your data if we legitimately think you will have an interest in using our product.

Lawful basis for processing

Our lawful basis for processing your data is a Legitimate Interest for marketing purposes. As you are a corporate entity, we also abide by the Privacy and Electronic Communications Regulations (PECR). We give you the chance to opt out of all marketing on anything that we send you. We only share details of our own goods and services in our marketing. If your data was not sourced directly from you, then we contact you once we have the data to let you know that we have your data and give you the chance to opt out. Our legitimate interest balancing test indicates that this is a legitimate purpose: you would not be surprised to hear from us based on the nature of your job role, and our processing does not cause any harm or risk to you as a data subject.

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. Where data is transferred outside of the EEA, we ensure that appropriate protection and mechanisms are in place, for example US Privacy Shield, or Standard Contractual Clauses. We do not sell your data to anybody.

Retention Periods

We hold data on Potential Corporate Clients for 5 years, or until the point at which you opt out of communications. At this point you are added to a suppression list so we do not contact you again. When you become a Corporate Client, then that Privacy Notice for will apply.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes. All devices are protected by leading enterprise mobility management technologies. We are IASME certified.

Investor/Shareholder Privacy Notice

Data that we hold and how we use it

As an investor or private shareholder in WIC, we hold your contact and investment details. This data will have been sourced directly from you in the course of your investment.

We use this data to pass to the regulators, to issue your share certificates and to manage our relationship with you.

Lawful basis for processing

Our lawful basis for processing your data is a legal obligation, contractual obligation and legitimate interest. Our legitimate interest balancing test indicates that this is a legitimate purpose; you would not be surprised to hear from us based on the nature of our relationship, and our processing does not cause any harm or risk to you as a data subject.

Data Sharing and Transfers

We share your contact details in line with our regulatory requirements, so will be listed in official documents such as company filings and would be used in any potential data room.

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. Where data is transferred outside of the EEA, we ensure that appropriate protection and mechanisms are in place, for example Standard Contractual Clauses. We do not sell your data to anybody.

Retention Periods

As a shareholder/investor we hold your information for as long as we are legally required to do so.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentification, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes.

3. Web Browsing Privacy Notice and Cookie Notice

Data that we hold and how we use it

As a web browser we collect information about you when you visit our website. This data includes information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our website that you visit, the time and date of your visit, the time spent on those pages and other usage statistics.

In addition, we use third party services such as Google Analytics that collect, monitor and analyse this data.

We use cookies solely to gather information on IP addresses, to analyse trends, administer the website, track your movements on our website and gather broad demographic information for aggregate use.

We are allowed to store cookies on your device if they are strictly necessary for the operation of Our sites. For all other types of cookies, We need your permission.

We ask you for consent to use cookies (where consent is required).

The cookies we use are as follows:

- On the WorkInConfidence web app / system we use only necessary cookies to enable you to have a good service:
- locale – stores the locale for the current user
- asideState – stores whether the function menu is open or closed
- trusted_device – stores whether you have enabled multi factor authentication
- PHPSESSID – the session details

On our marketing site we use cookies for the following::

- Leadworx to analyse use of our site
- Google Analytics to analyse use of our site
- A cookie to record whether you have accepted the cookie policy
- Bookify for arranging meetings.

Lawful basis for processing

For necessary cookies, we use legitimate interest as we need those cookies to exist for the website to work. For all other tracking we use consent. You can withdraw consent at any time by emailing dpo at workinconfidence.com

Data Sharing and Transfers

Like most companies, we use a number of other companies as part of our data processing, for example cloud services and technology services. We have Data Processing Agreements in place with these providers. Where data is transferred outside of the EEA, we ensure that appropriate protection and mechanisms are in place, for example Standard Contractual Clauses.

Retention Periods

We hold data on our web visitors for up to 6 months.

Technical and Operational Security

All data is password protected, access controlled by 2factor authentication, backed up securely and encrypted when appropriate. All employees are trained in data protection and are aware of their obligations to ensure the privacy of all data subjects. Data Privacy by Design and Default is an integral part of our development processes