



Willis Employment Services is committed to protecting the privacy and security of personal information.

This privacy notice describes how we collect and use personal data on behalf of current and former clients and others using our services, prospective clients, suppliers and visitors to our Willis Insurance & Risk Management Group website, in accordance with the General Data Protection Regulation (GDPR).

This notice does not form part of any agreement for services. We may update this Privacy Notice at any time. Please visit our website www.willisinsurance.co.uk if you want to stay up to date as our most recent Willis Employment Services Client & Supplier Privacy Notice will be available here.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

DATA CONTROLLER DETAILS

Willis Employment Services is a “data controller”. This means that we are responsible for deciding how we hold and use personal information. We are required under data protection legislation to notify the information contained in this Privacy Notice.

DATA PROTECTION PRINCIPLES

In relation to the personal data of you and employees working with you, we will:

- Process it fairly, lawfully and in a clear, transparent way.
- Collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you.
- Only use it in the way that we have told you about.
- Ensure it is correct and up to date.
- Keep your data for only as long as we need it.
- Process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed.

TYPES OF PERSONAL DATA WE PROCESS

CLIENTS AND PROSPECTIVE CLIENTS

To introduce and/or provide our advice and consultancy services to you we may collect, store, and use the following categories of personal information about you or employees working with you:

- Personal contact details including name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status.
- Dependants information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Job title.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, education history, employment history, references and other information included in a CV, application form or cover letter or as part of the application process).
- Employment records (including current and previous job titles, work history, working hours, training records, professional memberships and other terms and conditions relating to employment with our clients).



- Performance information (including performance management documentation, measurements against targets, formal warnings and related documentation with regard to capability procedures).
- Disciplinary and grievance information (including letters of concern, formal warnings and other documentation with regard to any formal procedure).
- Compensation history.
- Leave records (including annual leave, family leave and sickness absence).
- Health and Safety records (including training, compliance and accident/near-miss information).
- CCTV footage and other information obtained through electronic means such as building entry records.
- Photographs.
- Voice recordings.
- Vehicle tracking information.
- Social media identifiers and interactions.
- Information about your use of our information and communications systems, including IP addresses.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information used for equal opportunities monitoring about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.
- Biometric data used to uniquely identify an individual.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

SUPPLIERS

We don't collect much data about our Suppliers, only that which we need to make sure that our relationship runs smoothly. We will typically only personal contact information for individuals within your business, including name, title, addresses, telephone numbers, personal email addresses and job titles.

We may also collect personal bank details so that we can pay you where necessary and hold extra information that someone in your business has chosen to tell us.

CHILDREN

Our website and services are not aimed specifically at children. On occasion, where we are required to provide advice on an employment or workplace safety matter involving a child/children under sixteen (16), we will endeavour to do so in such a way that individual children cannot be identified. Should this not be possible, and where we do not rely on legitimate interests as our lawful basis for processing, we may seek consent from whoever holds parental responsibility for them.

HOW WE COLLECT YOUR PERSONAL DATA

We may collect data about you or employees working with you in a variety of ways including:

- Through provision of our advice and consultancy services to you, throughout which we may monitor and keep a record of that correspondence (in whatever form).
- During the course of dealings with you on behalf of a client, who will likely be your employer.
- When you provide us with information in relation to your attendance at any of our seminars or other hosted events.
- When you provide information to us by filling in forms on our Willis Insurance & Risk Management Group website or when attending an event.
- When we collect publicly available information about you or your business.
- When we collect your personal data from third parties such as employment agencies, former employers when gathering references, credit reference agencies, and, where agreed, from health professionals.



We collect a limited amount of data from visitors to our Willis Insurance & Risk Management Group website which we use to help us to improve your experience when using our website and to help us manage the services we provide. This includes information such as how you use our website, the frequency with which you access our website, and the times that our website is most popular.

WHY WE PROCESS YOUR PERSONAL DATA

We will only use personal information about you or employees working with you when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to supply our advice and consultancy services to clients, specifically our obligations as set out in our Service Agreement or as otherwise instructed by a client to a member of our Willis Employment Services team.
- Seeking advice from third parties in connection with your matter.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use personal information about you or employees working with you in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

For example, we need to collect personal information about you or employees working with you in order to:

- Invoice for and collect payments for services provided by us.
- Make payments for services provided by us.
- Market similar services to those currently provided to existing clients.

We also need to collect personal information about you or employees working with you to ensure we are complying with legal requirements such as:

- Health and safety obligations.
- Ensuring VAT is paid.
- Making reasonable adjustments.

Grounds for processing will overlap and there may be several grounds which justify our use of personal information about you or employees working with you.

Examples of situations in which we may process personal information about you or employees working with you are listed below:

- Providing clients and prospective clients with advice and consultancy services, including gathering evidence for possible grievance or disciplinary hearings, identifying relevant content for risk assessments, equal opportunities monitoring and performing behaviour audits.
- Representing clients in legal matters, specifically tribunal representation to include case preparation and conciliation.
- Seeking advice from third parties in connection with matters on behalf of clients.
- Business operations, management and planning, including workforce and task planning exercises.
- To prevent fraud.
- To prevent theft.
- To ensure our premises are secure, including preventing unauthorised access.
- To monitor your use of our information and communication systems.
- Keeping records of sources of work and new enquiries.
- Paying suppliers for services provided to us.
- Dealing with concerns and complaints.



SPECIAL CATEGORIES OF PERSONAL DATA

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- Explicit consent to the processing has been given.
- The data must be processed in order to carry out legal obligations.
- It is needed in the public interest.

Less commonly, we may process special categories of data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will use particularly sensitive personal information in the following ways:

- We will use personal information about employees working with our clients relating to leaves of absence, which may include sickness absence or family related leaves, to enable us to provide informed advice on sickness absence management procedures and to assist clients to comply with employment and other laws.
- We will use personal information, such as physical or mental health, or disability status, about employees working with our clients to enable us to provide informed advice on health and safety in the workplace and to provide effective guidance to employers in assessing fitness to work, providing appropriate workplace adjustments, monitoring and managing sickness absence and administering benefits.
- We will use personal information about employees working with our clients such as race or national or ethnic origin, religious, philosophical, political or moral beliefs, or sexual life or sexual orientation, to complete meaningful equal opportunity monitoring and reporting for our clients.

We do not need consent if we use special categories of personal data in order to carry out our legal obligations, exercise specific rights under employment law or to comply with regulatory obligations. However, we may ask for consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, whether a client or an employee working with a client, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

CRIMINAL CONVICTION PERSONAL DATA

We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is appropriate given the nature of the advice and consultancy services we are providing, where such processing is necessary to carry out our obligations and where the law permits us. This data will usually be collected when we are providing services to clients at the recruitment stage, however, may also be collected during employment.

We may use personal information in this way to assist clients in carrying out their obligations:

- To ensure compliance with relevant regulator guidelines in the UK.
- To satisfy Company car insurance policy obligations, and related claims.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where the information has been made public.

AUTOMATED DECISION MAKING

We do not envisage that any decisions will be taken about you or employees working with you using automated means (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you, however we will notify you in writing if this position changes.



IF YOU DO NOT PROVIDE PERSONAL DATA TO US

One of the reasons for processing personal information about you or employees working with you is to allow us to carry out our duties in line with a service agreement or alternative instruction to provide services to clients. If you do not provide us with the personal data needed to do this, we may be unable to perform those duties eg providing full and effective advice.

SHARING YOUR PERSONAL DATA

Personal information about you or employees working with you will be shared with colleagues within the Company where it is necessary for them to undertake their duties under your service agreement or alternative instruction to provide services.

We may share your personal data with third-party service providers including our IT services providers. This includes sharing your email address with our third party provider to deliver our e-newsletter.

We may share personal information about you or employees working with you with other entities in our group to complete a referral for additional services as instructed by you or for hosting of data.

All our third parties, including third-party service providers and other entities in the group, are required to take appropriate security measures to protect personal information in line with our policies and in accordance with the law. We only permit them to process personal data for specified purposes and in accordance with our instructions.

We may transfer some of your data outside of the EEA when specifically requested by individual clients and in the following instances:

THIRD PARTY TRANSFERS	PURPOSE	SAFEGUARDS IN PLACE TO PROTECT YOUR PERSONAL DATA
Eventbrite	To facilitate delegate registration at Company events	EU-US Privacy Shield
Facebook	To provide opportunities for engagement with our Company via our Company Facebook page	EU-US Privacy Shield
LinkedIn	To provide opportunities for engagement with our Company via our Company LinkedIn page and associated showcase pages	EU-US Privacy Shield
Twitter	To provide opportunities for engagement with our Company via our Company LinkedIn page and associated showcase pages	EU-US Privacy Shield
Salesforce	To manage marketing of our Company products and services	EU-US Privacy Shield

PROTECTING PERSONAL DATA

We have put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

HOW LONG WE KEEP PERSONAL DATA FOR

We will only retain personal information of you and employees working for you for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal or accounting requirements.



To determine the appropriate retention period for personal data, we consider 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 we process the personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Retention periods can therefore vary depending on why we need your personal data, as set out below:

MAXIMUM RETENTION PERIOD	TYPES OF PERSONAL DATA PROCESSED	RETENTION PERIOD DETAILS
Six (6) months	Equal opportunities information collected for the purposes of assisting clients to meet monitoring obligations	Six (6) months from the date of completion of the exercise
	Job applicant and equal opportunities information collected for the purposes of assisting clients to recruit	Six (6) months from the date of completion of the recruitment campaign
Seven (7) years	Personal data provided for the purpose of setting up and/or fulfilling our advice and consultancy service obligations	<p>To protect the Company in the event of any complaint or claim for breach of contract or professional negligence seven (7) years after:</p> <ul style="list-style-type: none">• the service agreement with us or you ends;• the date on which you request you no longer wish for us to provide you with services;• the date on which we request you no longer provide us with services;• completion of ad-hoc consultancy work. <p>If such a claim has been filed, the personal data will be retained for a period of seven (7) years following resolution of that claim and for seven (7) years following the resolution of any further claims.</p>
Twenty (20) years	Accident records and related documentation and records of consultations and correspondence with our consultants on the matter.	Twenty (20) years after the date recorded
Fifty (50) years	Health records for health surveillance, medical records relating to COSHH and lead and ionising radiation. Includes related documentation and records of consultations and correspondence with our consultants on the matter.	Fifty (50) years after the date recorded



Retention period cannot
be defined in advance

Risk assessments including related
documentation and records of consultations
and correspondence with our consultants on
the matter.

Permanently

In some circumstances we may anonymise personal information about you or employees working with you so that it can no longer be associated with the data subject, in which case we may use such information without further notice.

YOUR DUTY TO INFORM US OF CHANGES

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your business relationship with us.

YOUR RIGHTS IN RELATION TO YOUR PERSONAL DATA

Under certain circumstances, by law you have the right to:

- **Be informed.** This means that we must tell you how we use your personal data and the personal data of employees that you share with us, and this is the purpose of this privacy notice.
- **Request access** to your personal information. You have the right to access the personal data that we hold on you. To do so, you should make a subject access request: Our Subject Access Request Form is available on our Willis Insurance & Risk Management Group website.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Portability.** You can request we transmit personal data concerning you to another data controller, which you provided to us, in a structured, commonly used and machine-readable format, where technically feasible.
- **Not be subject to decisions that will have a significant impact on you based solely on automated decision-making**, unless we have a lawful basis for doing so and we have notified you.

In the limited circumstances where consent may have been provided to the collection, processing and transfer of personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Withdrawing your consent means that we will stop processing the personal data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the personal data where so permitted by having a legitimate reason for doing so.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our Operations Director in writing by email at peterl@willisinsurance.co.uk or by post to 55-59 Donegall Street, Belfast, BT1 2FH.

You will not usually have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.



willis
Employment
Services

CLIENT & SUPPLIER PRIVACY NOTICE

DATA CONTROLLER: WILLIS EMPLOYMENT SERVICES

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

MAKING A COMPLAINT

The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.

OPERATIONS DIRECTOR

Our Operations Director oversees compliance with our professional responsibilities and the reporting of any failures to comply with legislative requirements, including data protection. If you have any questions about this Privacy Notice or how we handle your personal information, please contact our Operations Director in writing by email at peterl@willisinsurance.co.uk or by post to 55-59 Donegall Street, Belfast, BT1 2FH.