



GDPR Privacy Notice & Retention Policy

What is the purpose of this document?

Howco Group Plc (Howco) is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR), as well as any other regional data protection laws in the countries we operate in.

It applies to all employees, workers and contractors.

Howco is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

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 protection principles

We will comply with data protection laws. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We may collect, store, and use the following categories of personal information about you:

- Personal details such as name, title, addresses, date of birth, gender, dependents, photographs, telephone numbers, personal email addresses, next of kin, and emergency contact information.



- Financial details such as your government issued identification number, bank account details, payroll records, tax status information, salary, annual leave, pension/retirement and benefits information.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV/Resume or cover letter or as part of the application process).
- Employment records (including start date, working location, job titles, work history, previous salary details, working hours, training records and professional memberships, performance, disciplinary, and grievance records (including in relation to expired sanctions)).
- Information about your use of our information and communications systems.
- CCTV footage and other information obtained through electronic means such as swipe-card records.

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

- Information about your race or ethnicity, religious beliefs, sexual orientation, marital status, and political opinions.
- Trade union membership, if applicable.
- Information about your health, including any medical condition, health and sickness records and genetic information and biometric data.
- Information about criminal convictions and offences.

How is your personal information collected?

We typically collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform any employment relationship or contract we have entered into with you.
2. Where we need to comply with a legal or regulatory obligation.
3. 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 your personal information in the following situations, which are likely to be rare:

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

Examples of situations in which we will use your personal information

- Making a decision about your recruitment or appointment, determining the terms on which you work for us and checking you are legally entitled to work in the location of which you are assigned.
- Paying you and providing you with benefits (including liaising with your pension/retirement provider) and, if you are an employee, deducting tax and/or any other legally required government required contributions.
- Business management and planning, including accounting, auditing, equal opportunities monitoring, and to conduct data analytics studies to review and better understand employee retention and attrition rates.
- Conducting performance reviews, managing performance, determining performance requirements, making decisions about salary reviews and compensation, and assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work, managing sickness and sickness absence, and complying with health and safety obligations.
- To prevent fraud, ascertain compliance with our policies and procedures, and ensure protection of our intellectual property.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law or regulation.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information.

The main reason we would need to hold and process these categories of information is to carry out our obligations as your employer.

We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our data protection policy.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension/retirement scheme, and in line with our data protection policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information 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 may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

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

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- Where applicable, we will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where a specific role(s) requires background checking, such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

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 you have already made the information public.

We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.



We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific employment law rights. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your employment relationship with us that you agree to any request for consent from us.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside your home location including the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: **payroll, human resource administration, pension/retirement administration, benefits provision and administration, IT services, legal services**. We may also share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

Transferring information outside your home location and/or the EU

We may transfer your personal information outside of your home location and/or the EEA for the purposes described in this policy. If we do this, we will use the appropriate safeguard of the model contractual clauses approved by regulators.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request from a member of the Human Resources team.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

Data retention

How long will you use my information for?

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

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with this data retention policy, and applicable laws and regulations.

Details of retention periods for different aspects of your personal information are outlined in the table below. Further information if required is available from our data privacy manager.

Type of Employee Data	Maximum Retention Period <i>Where information falls under more than one category the longest retention period will apply</i>
Job applications, CV/Resumes, background checks and interview records	<p><u>Unsuccessful candidates</u> – 6 months from notification</p> <p><u>Successful candidates</u> – 7 years after the date of termination of employment</p>
Criminal record checks and information about convictions and offences	<p><u>Pre-employment checks</u> – data will be deleted as soon as possible following recruitment/decision not to recruit (unless relevant to the ongoing employment)</p> <p>Information on spent convictions will be deleted as soon as possible after the conviction is spent (unless the employee is engaged in an excluded profession)</p>
<p>Key employment information:</p> <p>Including contracts of employment/written particulars of employment, commencement date, location of employment, work history, working hours, training records, performance information, disciplinary and grievance records, parental leave records, termination documentation and settlement agreements.</p>	7 years after the date of termination of employment
<p>Other employment information:</p> <p>Including records of family leave (maternity/paternity/SPL); working time opt-outs/ records to show compliance with the Working Time Regulations, hours worked, payments made to workers; immigration and right to work checks-</p>	7 years after the date of termination of employment
<p>Other Employment Information:</p> <p>Information regarding accidents or injuries in connection with work for regulatory reasons.</p>	7 years after the date of termination of employment or indefinitely where required by regulatory requirements

<p>Data not caught by other categories but containing:</p> <ul style="list-style-type: none"> • <i>Personal information:</i> Including name, title, gender, addresses, telephone number, personal email addresses, date of birth, copies of identification, photographs, bank account details, marital status and dependents, next of kin, and emergency contact information. • <i>Sensitive personal information:</i> Race, ethnicity, religious beliefs, sexual orientation, political opinions, Trade Union membership, health information including sickness records and genetic information and biometric data. • <i>Electronic information:</i> CCTV footage, swipe card records, information regarding use of information and communications systems including internet history. 	<p>7 years after the date of termination of employment or indefinitely where required by regulatory requirements</p> <p>CCTV records are kept for a period of 60 days</p>
<p>Remuneration information:</p> <ul style="list-style-type: none"> • including salary, payroll and wage records, tax records, government issued identification number, tax status information, annual leave, and pension/retirement and benefits information. 	<p>7 years after date of termination of employment</p>

Rights of access, correction, erasure, and restriction

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 working relationship with us.

Your rights in connection with personal information

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

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- 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 the 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 stop processing personal information where we are relying on a legitimate interest 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.
- Request the transfer of your personal information to another party.

You can exercise these rights by contacting the data privacy manager in writing.

No fee usually required

You will not 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.

What we may need from you

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).

Data privacy contact

If you have any questions about this privacy notice or how we handle your personal information, please contact a member of your regional Human Resource team or the Head of Human Resources & Compliance. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues or applicable governmental agency governing data privacy within your region.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the data privacy manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.