

GDPR, Privacy and Data Retention Policy

R G Wilbrey (Consultants) Limited understands that your privacy is important and that you care about how your personal data is used and shared. We respect and value the privacy of everyone and will collect and use your personal information to conduct our business, for employment requirements, to enable you to set up and operate an account with us, in order to enable you to access, use and/or purchase our services and products, to undertake surveys and for any other purpose referenced in the table in section 18 below. Your information may be shared with our associates and some third parties. Any personal data we do collect will only be used as permitted by law. Please read this Privacy Policy carefully and ensure that you understand it. Your acceptance of our Privacy Policy is deemed to occur upon your first use of Our Site and services. If you do not accept and agree with this Privacy Policy, you must stop using Our Site and services immediately.

1. Definitions and Interpretation In this Policy, the following terms shall have the following meanings:

“personal data” means any and all data that relates to an identifiable person who can be directly or indirectly identified from that data. In this case, it means personal data that you give to us via Our Site. This definition shall, where applicable, incorporate the definitions provided in the EU Regulation 2016/679 – the General Data Protection Regulation (“GDPR”); and

“We/Us/Our” means R G Wilbrey (Consultants) Limited, a limited company registered in England under company number No 797081, whose registered address is Aspen House, Great Brickkiln Street, Wolverhampton, West Midlands, WV3 0PT.

2. Information About Us

2.1 Our Site is owned and operated by R G Wilbrey (Consultants) a limited company registered in England under company number 797081, whose registered address is Aspen House, Great Brickkiln Street, Wolverhampton, West Midlands, WV3 0PT.

2.2 Our VAT number is 100573909.

2.3 Our GDPR point of contact is Fae Clough – Client & Supplier related data protection and can be contacted by email at fae.clough@rgwilbrey.uk.com by telephone on 01902 420920, or by post at Aspen House, Great Brickkiln Street, Wolverhampton, West Midlands, WV3 0PT.

2.4 We are regulated by NEBOSH, HIGHFIELDS, CITB, MHFA England, QUALSAFE, IOSH & UKATA for some of our training courses.

2.5 We are a member of BHSEA and a number of our advisors are Members of IOSH and OSHCR registered.

2.6 We are ISO 9001:2015 certified by Interface Limited, an accredited certification body, who carry out an annual audit to ensure compliance.

3. What Does This Policy Cover?

This Privacy Policy applies to all data collected and retained by R G Wilbrey (Consultants) Limited. We respect and value the privacy of everyone and will collect and use your personal information to conduct our business, for employment requirements, to enable you to set up and operate an account with us, in order to enable you to access, use and/or purchase our services and products, to undertake surveys and for any other purpose referenced in the table in section 18 below. Our site may contain links to other websites. Please note that we have no control over how your data is collected, stored, or used by other websites and we advise you to check the privacy policies of any such websites before providing any data to them.

4. Your Rights

4.1 As a data subject, you have the following rights under the GDPR, which this Policy and Our use of personal data have been designed to uphold:

4.1.1 The right to be informed about our collection and use of personal data;

4.1.2 The right of access to the personal data we hold about you;

4.1.3 The right to rectification if any personal data We hold about you is inaccurate or incomplete;

4.1.4 The right to be forgotten – i.e. the right to ask us to delete any personal data we hold about you (We only hold your personal data for a limited time, as explained in section 6 but if you would like us to delete it sooner. For the avoidance of doubt, we will only be able to remove the information we are not legally obliged to keep;

4.1.5 The right to restrict (i.e. prevent) the processing of your personal data;

4.1.6 The right to data portability (obtaining a copy of your personal data to re-use with another service or organisation);

4.1.7 The right to object to us using your personal data for particular purposes; and

4.1.8 Rights with respect to automated decision making and profiling.

4.2 If you have any cause for complaint about our use of your personal data, please contact us using the details outlined in this policy and We will do our best to solve the problem for you. If we are unable to help, you also have the right to lodge a complaint with the UK's supervisory authority, the Information Commissioner's Office.

4.3 For further information about your rights, please contact the Information Commissioner's Office or your local Citizens Advice Bureau.

5. What Data Do We Collect?

5.1 Depending upon your use of our services and Our Site, we may collect some or all of the personal and non-personal data.

6. How Do We Use Your Data?

6.1 All personal data is processed and stored securely In line with data retention as set out in the regulation and table below. We will comply with our obligations and safeguard your rights under GDPR at all times. For more details on security, see section 9, below.

6.2 Our use of your personal data will always have a lawful basis, either because it is necessary for our performance of a contract with you, because you have consented to our use of your personal data (e.g. by subscribing to emails), or use of services, employment reasons or because it is in our legitimate interests. Specifically, we may use your data for the following purposes:

- Supplying our services to you (please note that We require your personal data in order to enter into a contract with you);
- Personalising and tailoring our services for you;
- Replying to emails from you;
- Supplying you with emails that you have opted into (you may unsubscribe or opt-out at any time by emailing your request to fae.clough@rgwilbrey.uk.com),
- Market research
- Emailing or sending documentation relating to our contracted services.
- To fulfil employer obligations.

6.3 With your permission and/or where permitted by law, we may also use your data for marketing purposes which may include contacting you by email, telephone, post with information, news, and offers on our services. We will not, however, send you any unsolicited marketing or spam and will take all reasonable steps to ensure that we fully protect your rights and comply with our obligations under GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

6.4 You have the right to withdraw your consent to us using your personal data at any time, and to request that we delete it.

6.5 We keep your personal data In line with data retention as set out in the regulation. Data will therefore be retained for the following periods (or its retention will be determined on the following bases):

- Chat information will be retained for 30 days from the last date of contact, after which time it will be deleted.
- Chat enquiries will be passed to the relevant departments, and personal data will be kept by each department as defined in our Company Retention Policy detailed below in Section 18.

7. Sensitive Personal Data

7.1 In addition to the basic data described above, it may also benefit you to notify us when enrolling as a delegate of any health condition or disability you have, so that we are aware of these conditions and how they affect you. This will allow us to take any reasonable steps to accommodate specific needs or requirements you have when providing our services to you. This type of information is known under the law as ‘special category information’ (you may also know this as ‘sensitive personal data’) and we require your explicit consent to process this information.

7.2 This kind of information will only be collected from you and used by R G Wilbrey (Consultants) Limited to assist you, it will not be shared with any third parties and will only be kept as long as it is required for this purpose, or until such time as you notify us you no longer consent to it being held or processed by us.

8. How we collect data about you and your use of our services

You are in control of what information we collect about you. We may ask for information about you when you use our “Chat” facility or when you request brochures or other information. We may also invite you to complete surveys or provide us with feedback.

We collect information about your use of the website from cookies. For information about our use of cookies and how to decline them please read our Cookies Policy as set out in Section 17. We use your data to improve the service we offer you and to try and ensure that you get the best from our website. We will use the information you enter on the Chat facility for administration purposes.

In order to comply with our legal obligations, we will collect and store data relating to your employment with R G Wilbrey (Consultants) Limited as well as collecting any data necessary to provide the services as outlined in the contract with our clients.

9. How and Where Do We Store Your Data?

9.1 We only keep your personal data for as long as legally obligated and in line with our Retention Policy as set out in Section 18.

9.2 Your data will only be stored within the European Economic Area (“the EEA”) (The EEA consists of all EU member states, plus Norway, Iceland, and Liechtenstein).

9.3 Data security is very important to us, and to protect your data we have taken suitable measures to safeguard and secure data collected through Our Site, as part of providing service or for employment.

9.4 Steps we take to secure and protect your data include:

In cases where personal data is being processed by third parties, a rigorous adequacy process is being performed to ensure that your data is always secured.

- Web applications of R G Wilbrey (Consultants) Limited are operated in ISO 27001 certified secure data centres in the UK.
- Firewalls, anti-virus and anti-malware and backup and disaster recovery is in place to prevent data loss or deletion.
- Closed circuit television and door access control to authorised personnel secures the office.
- Access to infrastructure, elevated privileges and network are granted on an as-needed basis.
- Infrastructure and web applications operated by R G Wilbrey (Consultants) Limited is backed up on a regular basis and business continuity and disaster recovery is tested on a regular basis.
- All physical paperwork is locked away securely.
- Ensuring all Company IT equipment & mobile phones are password protected.
- All paperwork containing personal data no longer required is shredded or burnt.
- Ensure all our employees, clients & suppliers are aware of our Data Protection Policies.
- Ensure all employees have received training with regard to GDPR.

We will use all reasonable efforts to safeguard your personal information. However, you should be aware that the use of the Internet is not entirely secure and for this reason we cannot guarantee the security or integrity of any personal information which is transferred from you or to you via the Internet.

We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

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

10. Do We Share Your Data?

10.1 Subject to section 10.2, we will not share any of your data with any third parties for any purposes.

10.2 In certain circumstances, we may be legally required to share certain data held by us, which may include your personal data, for example, where we are involved in legal proceedings, where We are complying with legal obligations, a court order, or a governmental authority.

10.3 We may sometimes contract with third parties to supply services to you on our behalf. These may include payment processing, delivery of goods, Associate Health & Safety services AND/OR our Accredited Training Providers. In some cases, the third parties may require access to some or all of your data. Where any of your data is required for such a purpose, we will take all reasonable steps to ensure that your data will be handled safely, securely, and in accordance with your rights, our obligations, and the obligations of the third party under the law.

10.4 We may compile statistics about the use of our Site including data on traffic, usage patterns, user numbers, and other information. All such data will be anonymised and will not include any personally identifying data, or any anonymised data that can be combined with other data and used to identify you. We may from time to time share such data with third parties such as prospective investors, affiliates, partners, and advertisers. Data will only be shared and used within the bounds of the law.

10.5 The third party data processors used by us are located inside of the European Economic Area (“the EEA”) (The EEA consists of all EU member states, plus Norway, Iceland, and Liechtenstein).

11. What Happens If Our Business Changes Hands?

11.1 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, under the terms of this Privacy Policy, be permitted to use that data only for the same purposes for which it was originally collected by us.

11.2 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. When contacted you will be given the choice to have your data deleted or withheld from the new owner or controller.

12. How Can You Control Your Data?

12.1 In addition to your rights under the GDPR, set out in section 4, when you submit personal data to R G Wilbrey (Consultants) Limited, you may be given options to restrict

our use of your data. In particular, we aim to give you strong controls on our use of your data for direct marketing purposes. Should you wish to opt out of marketing emails, please contact: Rachael.Spence@rgwilbrey.uk.com.

12.2 You may also wish to sign up to one or more of the preference services operating in the UK: The Telephone Preference Service (“the TPS”), the Corporate Telephone Preference Service (“the CTPS”), and the Mailing Preference Service (“the MPS”). These may help to prevent you receiving unsolicited marketing. Please note, however, that these services will not prevent you from receiving marketing communications that you have consented to receiving.

13. Your Right to Withhold Information

You may access Our Site without providing any data at all. However, to use all features and functions available on Our Site you may be required to submit or allow for the collection of certain data.

14. How Can You Access Your Data?

You have the right to ask for a copy of any of your personal data held by us (where such data is held). Under GDPR, no fee is payable and we will provide any and all information in response to your request free of charge within 30 days of the request. Please contact us for more details using the contact details below in section 15.

15. Contacting Us

If you have any questions about Our Site or this Privacy Policy, please contact us by email at fae.clough@rgwilbrey.uk.com, by telephone on 01902 420920, or by post at Aspen House, Great Brickkiln Street, Wolverhampton, WV3 0PT. Please ensure that your query is clear, particularly if it is a request for information about the data we hold about you (as under section 14 above).

16. Changes to Our Privacy Policy

We may change this Privacy Policy from time to time (for example, if the law changes). Any changes will be immediately posted on Our Site and you will be deemed to have accepted the terms of the Privacy Policy on your first use of Our Site following the alterations. We recommend that you check this page regularly to keep up-to-date.

Questions, comments and requests regarding this privacy policy can be directed to the Company’s GDPR point of contact Fae Clough, email: fae.clough@rgwilbrey.uk.com, Postal address: R G Wilbrey (Consultants) Limited Aspen House Great Brickkiln Street Wolverhampton WV3 0PT, Telephone: 01902 420920

17. Use of Cookies

Like many websites, Our Site uses a technology called ‘cookies’, which are small computer files that are placed in your computer’s memory by the computer that provides or ‘hosts’ the website. Cookies are used to track data such as the total number of visits to the website. We use this information, which remains in aggregate form, to understand how our visitors use this website, so that we may improve the services we offer.

They help us to improve our website and to deliver a better service. Some of the cookies we use are essential for the website to operate. R G Wilbrey (Consultants) Limited does not use ‘cookies’ to collect personal identity information about you.

What is in a cookie?

A cookie is a simple text file that is stored on your computer or mobile device by a website’s server. Only that server will be able to retrieve or read the contents of that cookie. Each cookie is unique to your web browser. It will contain some anonymous information such as a unique identifier and the site name and some digits and numbers. It allows a website to remember things like your preferences or whether you are logged into a site to protect your privacy.

What to do if you do not want cookies to be set:

Some people find the idea of a website storing any information on their computer or mobile device intrusive, particularly when this information is stored and used by a third party without their knowledge. Although R G Wilbrey (Consultants) Limited cookies are quite harmless, you may not, for example, want to see advertising that has been targeted to your interests. If you prefer, it is possible to block some cookies, all cookies, or even cookies that have already been set; but you need to be aware that you might lose some functions of the website.

Web browser cookies

If you do not want to receive cookies, you can modify your browser so that it notifies you when cookies are sent to it or you can refuse cookies altogether. You can also delete cookies that have already been set.

If you wish to restrict or block web browser cookies which are set on your device then you can do this through your browser settings; the Help function within your browser should tell you how. Alternatively, you may wish to visit www.aboutcookies.org, which contains comprehensive information on how to do this on a wide variety of desktop browsers.

Strictly necessary cookies

Some cookies are strictly necessary in order to enable you to move around the website and use its features. Without these cookies, we will not be able to determine the number of unique users of the site or provide certain features.

Details of our Cookie usage:

WHAT THE COOKIE IS USED FOR & DETAILS	WHAT TYPE OF COOKIE?
Recognising you as a return visitor Using analytics software and a cookie, we can tell that you've visited the RGW website, which helps us understand what parts of the site you're coming back to see.	First-Party
Monitoring website traffic and video traffic We want to know which parts of our site are popular and which parts are less accessed, so we use a cookie to analyse traffic as it moves around the RGW website.	First-Party (including Google) and Third-Party
Reminding you of RG Wilbrey elsewhere Many third parties such as weblogs, newspapers, search engines and other sites online will use a cookie to check if you've visited the RGW website lately, as part of a service that we use. If you have visited us, the third party will show you an advertising message on their website.	Third-Party (including Google)
Understanding how people found us We want to know how our website caught your eye, so we use a cookie to understand how you found the RG Wilbrey website when you visit.	Third-Party (including Google)
Offering a live chat facility If you have a question about the RG Wilbrey website, we can quickly answer it using a live chat on the website. We use a cookie to remember whether you closed the live chat box so we won't show it again.	First-Party / Third Party

18. Data Retention Policy

This Policy sets out the obligations of R G Wilbrey (Consultants) Limited regarding data protection and the rights of employees, contractors, associates, clients training delegates, business contacts and service providers (“**Data Subjects**”) in respect of their personal data under GDPR.

Under GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purpose of processing or as required to be retained by law.

Aims and Objectives

The primary aim of this policy is to set out limits for the retention of personal data and to ensure that those limits are adhered to. By extension, this Policy aims to ensure that the Company complies fully with its obligations and rights of data subjects under GDPR.

In addition to safeguarding the rights of data subjects under GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the managing of data.

Scope

The Policy applies to all personal data held by R G Wilbrey (Consultants) Limited and/or HR, contractual business, marketing, enquiry and provisions of services purposes and by third-party data processors processing personal data on the Company’s behalf.

Personal data, as held by the Company OR third-party is stored in the following ways and in the following locations:

The Company’s servers, located at the Company’s registered address;

Third-party servers, operated by Microsoft, Office365, NEBOSH, HIGHFIELDS, CITB, UKATA, IOSH and SAGE and located in areas as outlined in their Data protection/Privacy Policies.

Computers permanently at the Company’s registered address;

Laptops and other mobile devices provided by the Company to its employees;

Physical records stored in each department, within locked filing cabinets and store cupboards;

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects’ rights thereunder, as set out in the Company’s Data Protection Policy.

18.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used and how long the Company

will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

18.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, and further rights relating to automated decision-making and profiling.

19. Technical and Organisational Data Security Measures

19.1 The following technical measures are in place within the Company to protect the security of personal data:

- a) All emails containing personal data must be encrypted;
- b) All emails containing personal data must be marked "confidential";
- c) Personal data may only be transmitted over secure networks;
- d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
- e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
- f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
- g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using Royal Mail or Parcelforce;
- h) All personal data transferred physically should be transferred in a suitable container marked "confidential";
- i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from our GDPR points of contact:
Fae Clough – Health and Safety Advisor Email: Fae.Clough@rgwilbrey.uk.com
- j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

- k) No personal data may be transferred to any employees, agents, associates, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;
- l) Personal data must be handled with care at all times and should not be left unattended or on view;
- m) Computers used to view personal data must always be locked before being left unattended;
- n) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of Louise Farlow and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to associates, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;
- p) All personal data stored electronically should be backed up daily with backups stored onsite AND/OR offsite. All backups should be encrypted;
- q) All electronic copies of personal data should be stored securely using passwords and encryption;
- r) All passwords used to protect personal data should be changed regularly and should must be secure;
- s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do have access to passwords and should be informed of any changes;
- t) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;
- u) No software may be installed on any Company-owned computer or device without

approval; and

v) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Line Managers to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

19.2 The following organisational measures are in place within the Company to protect the security of personal data:

- a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy and relevant Privacy Policies;
- b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;
- c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;
- e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
- f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;
- i) All associates, agents, contractors, or other parties working on behalf of the Company

handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

j) Where any associate, agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

20. Data Disposal

Upon the expiry of the data retention periods set out below in Section 18 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

20.1 Personal data stored electronically (including any and all backups thereof) shall be deleted securely;

20.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely;

20.3 Personal data stored in hardcopy form shall be shredded or burnt. Large quantities of shredding will be disposed of by a GDPR compliant shredding company;

6.4 Special category personal data stored in hardcopy form shall be shredded or burnt. Large quantities of shredding will be disposed of by a GDPR compliant shredding company

21. Data Retention

21.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

21.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below and within the RGW HR Privacy Policy and RGW Personal Data Processing Activities document.

21.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;

- b) The type of personal data in question;
- c) The purpose(s) for which the data in question is collected, held, and processed;
- d) The Company's legal basis for collecting, holding, and processing that data;
- e) The category or categories of data subject to whom the data relates;
- f) The duration of projects in relation to documentation and site inspections.

21.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

21.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

21.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by GDPR.

22. Data Retention Table

The personal data collected shall be processed for the following purposes and on the following legal basis as set out in the table below.

Data processed	Purpose	Legal basis (Art. 6 GDPR)
- Name and surname; - E-mail address; - Telephone number; - Date of birth or address; - National Insurance number; - relevant training Certificates; - Work permits/Right to work documents; - Other official documents such as your driver's license or other relevant documents; - Your bank account; References; Your attendance information	Providing the Service stipulated in the Terms of Business, in order to comply with employer obligations, to provide HR support and managing all the necessary issues for its maintenance, for which these data are strictly necessary.	Necessary for the performance of the contract (Art. 6.1.b GDPR).
- Name and surname; - E-mail address; - Telephone number;	Sending promotional information related to the training/courses you have activated, such as training courses related to your professional activity.	Necessary for the performance of the contract (Art. 6.1.b GDPR) and for legitimate interest (Art. 6.1.f GDPR).
- Name and surname; - E-mail address; - Telephone number; - Address in certain circumstances	Sending promotional information which is not related to the main activity of RGW: third party updated such as regulation updates.	Consent (Art. 6.1.a GDPR).
- Name and surname; - E-mail address; - Telephone number; - Date of birth; - relevant training Certificates; - Work permits; - Other official documents such as your driver's license or other relevant documents;	Automated decision-making including profiling related to the activity of providing and applying for courses.	Necessary for the performance of the contract (Art. 6.1.b GDPR)..
-Relevant training Certificates; - Work permits; References; - Other official documents such as your driver's license or other relevant documents;	Professional references of the person with the purpose of improving the competencies of the person. More information in section 6 of the General Terms of Use.	Legitimate Interest (Art. 6.1.f GDPR).

- The date and time of the visit and the duration of the use of the website; - The IP address of your device; - The referral URL (the website from which you may have been redirected); - The subpages of the website visited; and - Further information about your device (device type, browser type and version, settings, installed plug-ins, operating system).	Processing of the usage data to enable you to use the website and to ensure the functionality of the website. In addition, we process usage data to analyse the performance of the website, to continuously improve the website and correct errors or to personalise the content of the website for you. We also process the usage data to ensure IT security and the operation of our systems and to prevent or detect misuse, especially fraud.	Legitimate Interest (Art. 6.1.f GDPR).
- Name and surname; - E-mail address; - IP Address	Enable registering as a User.	Necessary for the execution of the contract (Art. 6.1.b GDPR)..
- Name; - E-mail address; - IP Address	Enable the posting of personal content to RGW.	Consent (Art. 6.1.a GDPR).
- relevant training Certificates; - Work permits; - Other official documents such as your driver's license or other relevant documents;	Use feedback from the User's former employers to determine whether he/she is suitable for the applied job.	Necessary for the performance of the contract (Art. 6.1.b GDPR).
- Name and surname; - National Insurance number; - Work permits; - Other official documents such as your driver's license or other relevant documents;	Complying with our legal obligations for purposes such as Tax and Accounting	
Data processed depends on the case however it typically may involve: - Name; - Surname; - Email address; - Address; - Feedback and references of former employers and of clients that the workers worked for; - Banking information;	The assertion or defence of legal claims on RG Wilbrey (Consultants) Limited's part.	Legitimate Interest (Art. 6.1.f GDPR).

23. Roles and Responsibilities

The Company's GDPR point of contact is our Health and Safety Advisor, Fae Clough. Contact Details: By email: Fae.Clough@rgwilbrey.com, by telephone: 01902 420920, or by post: at Aspen House, Great Brickkiln Street, Wolverhampton, West Midlands, WV3.0PT.

The GDPR point of contact shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data

Protection related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

The Line Managers shall be directly responsible for ensuring compliance with the above data retention periods within their departments.

Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the GDPR point of contact as detailed in section

Implementation of Policy

This Policy shall be deemed effective as of 17th June 2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.