

This privacy notice explains the processing of personal data of customers and former customers of Assurity Consulting Ltd (including the entity of Assurity Consulting Holdings Ltd).

Topics:

Why do we process your personal data?

What are the principles we apply when processing your personal data?

What types of data do we process?

What are the lawful bases for processing the data?

How long will we retain your personal data?

Who is the data controller and who processes your data?

What are your rights as a data subject?

Changes to this privacy notice.

How to contact us?

Why do we process your personal data?

We need to collect and process information about you (personal data) as a customer for many reasons including but not limited to:

- communication by phone/email;
- supplying documents relevant to our contract with you;
- informing you of our events and seminars;
- updating you with important information relevant to your business role and communications relating to finance operations;
- undertaking authorised assessments e.g. DSE assessments and reports; and
- registering you for our events (we will share your name with the venue for security reasons).

We need to collect data and process information (personal and company data) on our online compliance system Assurity Plus when we engage with you under a contractual agreement and you become our customer. The reasons for processing the data include but are not limited to:

- Setting up access to Assurity Plus;
- Accessing data stored on Assurity Plus to view and manage reports produced by us and upload reports from Customers and Contractors into the actions section of Assurity Plus;
- Accessing and managing documents uploaded to the Document Library of Assurity Plus; and
- Providing support with the management of data stored on Assurity Plus on your behalf.

If you wish to share any special category data with us then this should be agreed with us in advance so that we can put any additional controls required in place to minimise and protect the storage and dissemination of this data.

We will only access special category data if you have signed an agreement allowing us to do this. Please also see our privacy notice 'Assurity Plus Incident Reporting and Incident Management Privacy Notice'.

What are the principles we apply when processing your personal data?

As a responsible business we apply and are able to demonstrate compliance with the following principles to our control and processing of personal data relating to you as a customer or a former customer:

- Processed lawfully, fairly and in a transparent manner in relation to customers;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Processed in a way that is adequate, relevant and limited to what is necessary;
- Maintained to ensure it is accurate and where necessary kept up to date. Every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed is erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

We take reasonable steps to ensure that 3rd parties who process data on our behalf also apply and are able to demonstrate compliance with the above principles.

What types of data do we process?

The following list is not exhaustive, but will give you an idea of the kinds of data we may process relating to you. This list will be reviewed regularly as part of the review of this privacy notice to make sure it is as complete as possible:

- Name;
- Salutation;
- Gender;
- Job title;
- Site address;
- Company name;
- Personal phone number;
- Company phone number;
- Personal email address;
- Company email address;
- Company policies and procedures;
- Risk assessments;
- Method statements;
- Training certificates;
- Contract letters;
- Reports and communications;

- Emails that you send or receive or are copied or blind copied in;
- Communications from external authorities relating to the company – such as Environmental Health Officer letters and inspections; and
- Communications from 3rd party suppliers eg service and maintenance reports

3rd party data that you supply

- Persons name;
- Salutation;
- Company name;
- Job title;
- Company phone number; and
- Company email address.

What are the lawful bases for processing the data?

Customers

For customers the act of you entering into a contract is your agreement for us to process your data purely for the purposes of the contractual agreement. We will also process your data to send you information which we believe will be of interest to you and to enable access to your reports. This may include invites to seminars, health and safety updates and setting up access to Assurity Plus, etc.

For customers we process your data to perform the contract between you and us. Some processing of data is directly related to performing our contract others may be for the processing of invoicing and the use of Assurity Plus. This may require the holding of different peoples personal data.

Where specifically requested by the customer we will process your data by uploading our reports to an electronic platform of your choice.

Former customers

If you leave your company your personal information will be deleted from our accessible customer management systems and stored in our secure storage area.

If our contractual agreement ends we will not process any customer personal data on Assurity Plus. However, we will hold any reports produced by Assurity Consulting containing customer personal data for 40 years to comply with our professional indemnity insurance. Much of the longer term retention of data will be on the grounds of legitimate interests to defend legal and insurance claims both on behalf of us and our suppliers and customers.

In this case, we will provide you with electronic data exported from Assurity Plus and access for your company to Assurity Plus will be ceased after 1 year of the contractual agreement ending.

Invoicing and order records will be kept for 7 years to comply with our legal requirement. This is in line with our Data Protection and Privacy Policy.

Marketing purposes

As a customer by not opting out of our marketing communications, you are allowing us under the basis of legitimate interest to process your data for the purposes of sending you up to date email information or calling you about health, safety and environmental topics:

- Educational white papers;
- Up to date industry news;
- Assurity Consulting business and services updates; and
- Invitations to our educational seminars and webinars.

The information we send to customers via email is written by experts from an education stand point. For example, we send our customers emails on a monthly basis and these can be opted out of at any time:

- Workplace Compliance News – 5 current news articles on health, safety, or environmental subjects relevant to our customer base.
- Workplace Compliance Alert – topic based on email and white paper/s, based on health, safety or environmental information or legislation that our customer base would appreciate being informed about.

How long will we retain your personal data?

Where there is an outstanding dispute, court proceedings, legal claim, insurance claim, or similar we will extend the retention periods stated below of data relevant to the case until the case is closed and the window of opportunity to appeal any decision is considered to be closed.

Current customers

We will keep relevant data throughout the duration of your contract with us. You have a duty to inform us of changes, such as changes to any personnel and their data. We will ensure that we keep your records up to date based on the updates you have provided.

Former customers

- Within 1 year of your contract with us expiring
We will provide you electronically with all the data held on Assurity Plus relevant to your portfolio. After this period this data will be no longer available to you on Assurity Plus. All your data will be deleted from Assurity Plus.
- Within 7 years of us delivering our last piece of work to you

Quote documents, contract/contract renewal documents, other customer letters and customer e-mails will be kept for a maximum of 7 years. This will also include letters and emails that you have sent to consultants or been copied in on that provide requests or feedback on advice, scope of works, quotations for work etc. Such correspondence may be deleted as required as per our customer or supplier privacy notice guidelines.

- Within 40 years

On the advice of our liability and professional indemnity insurers, customer reports and customer advice documents will be retained for up to 40 years. This information can contain your name if you were the person who was responsible for the building.

Asbestos related data will also be kept for up to 40 years. We will also keep your name and last job title for up to 40 years after you cease to be a customer.

Data back-ups

To protect our business interests we undertake secure back-ups of our data. As these back-ups are formed of disc images it is not realistic for us to delete or search for individual data items in these back-ups. However, we limit our back up retention to 12 months so within 13 months after the retention guidelines given above, the data will also have been removed from our back-up systems.

We will keep a list of people who have asked for the right to erasure or the right to restrict processing only for the purposes to ensure they are not contacted within the terms set out in the privacy policy.

Who is the data controller and who processes your data?

We are the data controller but third parties may also control the data if required for the customers own invoicing system or reporting platform. This will require written consent from the customer concerned.

We have our own in house Finance function and so we also process much of the required personal data for the purposes of maintaining the contract.

We have our own in house Consultancy Services and Customer Administration teams who process your data on Assurity Plus for the purposes of maintaining the contract agreement. Access rights for our employees are maintained so that only those employees who support your account have access to your data.

We have our own in house marketing team and CRM system so we process much of the required personal data for the purposes of marketing our information to you. However, there are some EU based third parties that we may need to send your data to and from, or may view your data for processing, these include but are not limited to a:

- Marketing agency;
- Website agency;

- Direct marketing consultancy;
- Search engine optimisation consultancy;
- Mass email marketing company;
- Survey company; and
- Venue where we host our events

However, as part of our contract agreement with you we will not provide access to Assurity Plus to a third party unless instructed by you to do so.

When personal access rights to Assurity Plus are granted to a customer, the **customer** becomes the **data controller** and needs to adhere to their own Data Protection Policy.

Where Assurity Consulting reports are uploaded to a 3rd party platform, we will not be the data controller.

It may sometimes be necessary to transfer your personal information overseas. When this is needed information is normally only shared within the European Economic Area (EEA). Our main data servers are located in the UK and maintained by a UK based data storage company. Data may be transferred outside of the EEA by the data storage company as part of their support provision to ensure continuity of service. We have a contract in place with the data storage company to ensure that the highest data security standards are maintained. Any transfers made will be in full compliance with all aspects of the Data Protection Act.

What are your rights as a data subject?

If you would like to realise any of these rights please contact us using the contact details provided in the "how to contact us" section of this document. Please make it clear what right you want to realize and be as specific as possible with what you want so that we can prioritise your request.

Right to be informed – you have the right to be informed about how and why we process your personal data. This privacy notice is designed to meet this requirement.

Right of access – you have the right to access your personal data that we hold on you. If you make a request please try and be as specific as possible about the type of data you would like to have access to and the time frames you would like us to look at. We may contact you to discuss your request to help to meet your needs.

Right to rectification – you have the right to request that we rectify your personal data. We also want to make sure that your personal data is accurate and up to date. Please let us know if there is data about you that you believe is incorrect and needs to be rectified.

Right to erasure (to be forgotten) – you have the right to request the deletion or removal of personal data. We believe that we have set out clearly the data we hold, the legal bases for processing the data and a realistic retention period which balances the rights of you as an individual against the interests of us and third parties. However,

if you believe that we have data on you that should be deleted, please let us know, so that we can investigate.

Right to restrict processing – you have the right to request that we ‘block’ or suppress processing of data (including deletion of data). If you wish to exercise this right please let us know the reasons for this.

Right to object – you have a right to object to our processing of your personal data. If you wish to exercise this right please give clear details on the grounds of your objection.

Right to data portability – We do not believe that we hold data on our customers that falls into the definition of this right within the GDPR regulations. However if you believe we are incorrect please let us know why and what data you believe we should enable for portability.

Rights related to automated decision making including profiling – you have a right to be informed that profiling or automatic decision making will be performed, right of access to things like the logic involved in automatic decision making, right not to be subject to a decision based solely on automated decision making. If we wish to profile your data or automate decisions based on your data we will let you know as soon as possible.

Right to lodge a complaint with a supervisory authority – you have the right to raise a complaint with the supervisory authority in the country where you live, where you work, or where the infringement took place. In the UK the supervisory authority is the ICO (ico.org.uk).

Changes to this privacy notice

We regularly review our privacy notices. The most up to date privacy notices are available on our website. The date of issue of this privacy notice is indicated in the footer of the document.

How to contact us?

If you have any questions about this privacy notice or the personal data we hold about you, please contact us as follows:

Email: dataprotection@assurityconsulting.co.uk

Write: Data Protection Compliance Coordinator
Assurity Consulting Ltd
26 Redkilyn Way
Horsham
West Sussex
RH13 5QH