This privacy notice explains the processing of 3rd party data as part of a contract that we have with a customer (or former customer) of Assurity Consulting Ltd (including the entity of Assurity Consulting Holdings Ltd).

Topics:

Why do we process your personal data?

Most of the data we process as part of a contract with our customers is covered in our *Customer Privacy Notice* that is available on our website.

Where our customers process your data and store it on the Assurity Plus Incident Reporting Module or the Assurity Plus 2.0 Incident Management Module please in the first instance refer to the privacy notices supplied by our customer as they are the Data Controller in this instance. This is also covered in our capacity as Data Processor in our *Assurity Plus Incident Reporting and Incident Management Privacy Notice* that is available on our website.

However, there will be times when we need to process your data as part of the work we undertake for our customers.

If you have been allocated a specific role, task, position of responsibility, etc. by our customer for some aspect of health, safety, environment, maintenance of their property or workplace then we may need to include your name, and other work related personal data as part of a report for a customer for which it is directly relevant.

There are also work types where we will need to process your data if you are the specific subject of the work we are undertaking. This could include more sensitive special category data such as health data where this is specifically required to complete our work for the customer to a suitable and sufficient level of detail. These work types include the following (although we are evolving what we can deliver to our customers all the time):

- Display Screen Equipment (DSE) Assessments in person at your place of work;
- Remote DSE Assessments and follow-up including home based DSE assessments;
- Accident and incident investigations, including RIDDOR reporting;
- New and Expectant Mothers Risk Assessments;
- Return to work assessments and risk assessments;

- Health surveillance work (e.g. Noise exposure);
- Personal Emergency Evacuation Plans (PEEPS);
- Support with Access Audits and Arrangements;
- Interviews to support a management review of Health and Safety arrangements;
- Providing Training (delegate information, invites, tests, feedback, and certificates);
- Workplace Environment Assessment of a building where testing is required around where you work due to health conditions or a complaint etc; and
- Receiving enquiries from customers and responding and providing advice were this is specific to you as a named person.

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:

- Processed lawfully, fairly and in a transparent manner;
- 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 lists are not exhaustive, but will give you an idea of the kinds of data we may process relating to you. These lists will be reviewed regularly as part of the review of this privacy notice to make sure it is as complete as possible.

The data we process may be collected from you directly as part of our work with a customer by meeting with you, phoning you, corresponding with you etc., or it may be supplied by our customer to us. We will never request any access directly of your medical records or records from other authorities about you, except where this is in the public domain such as an industry body list of those who hold specific qualifications.

If you have been allocated a specific role, task, position of responsibility, etc. by our customer for some aspect of health, safety, environment, maintenance of their

property or workplace then the following kinds of data may be processed where relevant:

- Name;
- Salutation;
- Gender;
- Job title;
- Site address;
- Company name;
- Company phone number;
- Company email address;
- Qualifications and training certificates (relevant to your nominated role); and
- A description of your role, allocated tasks, position of responsibility, etc.

If you are the specific subject of the work we are undertaking then the following kinds of data may be processed where strictly relevant to the piece of work we are undertaking:

- Name;
- Salutation;
- Gender;
- Job title;
- Work location/address;
- Working hours, shift pattern, or workload;
- Work history (positions, responsibilities, and dates etc.);
- Work activities you undertake (to help with risk assessments);
- Company name;
- Company phone number;
- Home/personal phone number (only where strictly required such as a home based DSE assessment follow-up by phone where you do not have a company mobile, or have no coverage of the company mobile when at home etc)
- Company email address;
- Personal email address (only where strictly required where you do not have access to a relevant work email address for the purposes of our work);
- Qualifications and training certificates (relevant to your nominated role);
- A description of your role, allocated tasks, position of responsibility, etc.;
- Photo or video of your home workstation (provided by you);
- Your home address (only if legally required, such as on a standard accident form or if this is your fixed place or work etc.);
- Photographs of an accident or incident scene; and
- Previous reports on you from our customer, such as info of previous DSE assessments, previous accident or incident investigations.

As part of this work we may also need to process some special category data about you in order to complete the specific work. We will only process data that is relevant to the work we are doing. In the main this special category data will relate to your health such as:

- Symptoms you have (such as pain);

- Diagnoses of relevance (such as sciatica for a DSE assessment, gestational diabetes for a New and Expectant Mothers Risk Assessment);
- Treatment or care plan in place for symptoms, diagnoses, conditions;
- Equipment or auxiliary aids that you are using, or have available to you (such as a Bariatric chair, walking frame, DSE equipment);
- Stressors that you are exposed to (such as noise, slow broadband, colleague relationships);
- Background story (what lead up to an accident, what you have already tried to make a workstation more comfortable);
- Copies of medical letters directly relevant to situation;
- Time of work and general sickness records from your employer;
- Details and/or photographs of an injury;
- Details of disabilities (for work such as access audits and PEEPs); and
- Details of any limitations in undertaking certain tasks.

What are the lawful bases for processing the data?

First and foremost we will not process your data as described above unless we have a contract in place with our customer and are processing your data on behalf of our customer as part of that contractual agreement. In the main our customer will be the Data Controller and we are a Data Processor working on their behalf under contract.

As part of our contract with our customer for this kind of work we will expect that our customer will have a privacy notice to cover this data processing and will explain in detail the legal bases for them processing your data. Where you are the employee, worker, or contractor of a customer the primary legal basis of our customer processing your data will likely be to perform the contract of employment or contract of service or contract for services between you and our customer.

Where we process your special category data (medical information disclosed as part of accident, incident, sickness, etc. records) our customers privacy notice will indicate the condition of processing such data. It is likely that this will be under the 'employment, social security and social protection law' condition of processing.

For the avoidance of doubt, in the rare instances where we might be joint data controllers with our customer the condition of us processing your special category is 'employment, social security and social protection law' condition of processing.

There are many laws that require this processing of data. The Social Security (Claims and Payments) Regulations requires that accident records are kept. The Health and Safety at Work, etc. Act 1974 requires employees to co-operate with employers to enable them to fulfil their statutory duties, including reporting all dangerous occurrences, near misses and accidents whether or not they resulted in injury, damage, or disease. The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations requires us as an employer to report certain defined work-related events to the enforcing authority.

Through our contract with our customer we are supporting our customer in their role as Data Controller for the above.

We will keep a copy of advice and reports supplied to a customer to help us provide the best support to our customer but to also defend any legal claim against us or to help support a claim through liability or professional indemnity insurance.

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 or contest any decision is also 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?

For most of the work we do, where customers are asking for support for their employees, workers, our **customer** is the **data controller** responsible for managing access to your data. It is our customer's responsibility to make the data subject (a person) aware of how your data is processed, the lawful bases for this processing, the data retention periods, the rights of the data subject etc. Where the customer decides to process special category data such as medical information, they will also need to provide the data subject with details of the conditions of processing.

In some instances it is possible that our customer will be joint data controllers with us for some aspect of your data. This privacy notice aims to make you aware set out how your data is processed, the lawful bases for this processing, the data retention periods, the rights of you as a data subject etc. Where we need to process your special category data such as medical information, we have also provided details of the conditions of processing.

Where Assurity Consulting reports are uploaded to a 3rd party platform, we will not be the data controller or joint 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 in the first instance contact the data controller (our customer). Usually you will be able to find details of how to make contact on their website or in the relevant privacy notice. You can also search the public register on the Information Commissioner's Office (ICO) website for details of how to make contact. For the instances where we and our customer are joint data controllers, then please also see the how to contact us section below.

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 Redkiln Way
Horsham
West Sussex
RH13 5QH