This privacy notice explains the way we process and access personal data of customers that use the Assurity Plus Incident Reporting Module or Incident Management Module provided by Assurity Consulting Ltd (including the entity of Assurity Consulting Holdings Ltd) as a part of a contractual agreement.

Topics:

Why do we process your personal data?

The Incident Reporting Module and Incident Management Module on Assurity Plus are used to collect, access and process personal information about a customer employee, third parties working for a customer, visitors, members of the public, pupils, students, or any other party that engage with a customer as a part of their business operations for many reasons but not limited to:

- a customer entering accident data on to the Incident Reporting Module or Incident Management Module or our employees carrying out this task as a part of a contractual agreement;
- the collection of electronic accident data so that the Incident Reporting Module or Incident Management Module becomes a customer's central repository for this information;
- the review of accident related data and trends by a customer or our employees as a part of a contractual agreement; and
- the defence of personal injury insurance claims or court cases relating to liability or professional indemnity.

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 individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; [for the Incident Reporting Module and the Incident Management Module the majority of the data is collected by our customer who is the data controller]

- 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.

In relation to personal data processed on Assurity Plus we will not provide access for any third parties unless specifically requested by the customer. The only exception is our vetted development partner who we use for the development of our Assurity Plus system. We have taken reasonable steps, to ensure they are able to demonstrate compliance with the above principles.

What types of data do we process?

We will not be able to process the data or provide access to a third party (apart from our supplier used for the development of the system) unless you have signed an agreement to allow nominated employees to access the Incident Reporting Module or the Incident Management Module.

The following list is not exhaustive, but provides an overview of the type of data that may be processed on the Assurity Plus Incident Reporting Module or the Incident Management Module. In some instances where a medical condition is an underlying cause of an incident this may need to be recorded by our customers to show that all the circumstances have been considered and investigated adequately. Such medical information is likely to be special category data as defined by the Data Protection Act and may be more sensitive than the other data recorded. 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;
- Date of birth;
- Home address;
- Personal phone number;
- Company phone number;
- Details of the incident, its time and location;
- Details of injuries sustained;
- Investigation reports;
- Witness statements;

- Photographs of a person or a location where the accident occurred;
- Sickness and absence records, doctors certificates, medical letters and return to work meeting notes;
- Disciplinary and grievance evidence, investigations, and hearing minutes;
- Written warnings, final written warnings, and performance management letters;
- Review meeting notes and personal development notes and actions;
- Emails that are sent or received or are copied or blind copied in; and
- Communications from external authorities relating to the incident – such as EHO post visit observation letters, improvement notices speeding offence letters from the police.

What are the lawful bases for processing the data?

Customers
We will only process customer data on the Assurity Plus Incident Reporting Module or the Incident Management Module for the fulfillment of a contractual agreement between the customer and Assurity Consulting Ltd.

We will only access customer data on the Assurity Plus Incident Reporting Module or Incident Management Module if there is a signed agreement with the customer.

Former customers
We will not process any personal customer data on the Assurity Plus Incident Reporting Module or Incident Management Module if our contractual agreement has ended. In this case, we will provide you with the data export from Assurity Plus and access for your company to Assurity Plus will cease after 1year of the contractual agreement ending.

How long will we retain your personal data?

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

Former customer:

- 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.

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?
Assurity Consulting employees, apart from our IT team, as a default will not be able to access data stored on the Incident Reporting Module and the Incident Management Module. Access will only be granted to Assurity Consulting employees after receiving a signed agreement from the customer.

If access to the Incident Reporting Module or Incident Management Module is not requested or granted by the customer, Assurity Consulting employees will not access the data processed. Therefore, the **customer** is the **data controller** responsible for managing access to the Incident Reporting Module or the Incident Management Module for their employees. It is the customer's responsibility to make the data subject (a person) aware of how their incident 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.

The only 3rd party that may access your data from the Assurity Plus Incident Reporting Module and the Incident Management Module is our support provider used for the development of the system. All data is held on cloud storage, managed by a third party data processor (UK based). We have a separate contract agreement with this supplier which details how they process and access data.

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 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 Commisioner's Office (ICO) website for details of how to make contact.

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. Please also see the privacy notice or equivalent that the data controller issues regarding this processing of data.

Right of access – you have the right to access your personal data that is held on you.

Right to rectification – you have the right to request that incorrect data held about you is rectified.

Right to erasure (to be forgotten) – you have the right to request the deletion or removal of personal data.

Right to restrict processing – you have the right to request the suppression of data processing(including deletion of data).

Right to object – you have a right to object to the processing of your personal data.

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.

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 , 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