
Effective Date: 4 August 2026

Last Updated: 4 August 2026

This privacy notice explains the way we process and access personal data of customers and, suppliers to our customers, that use the Assurity Plus 2.0 Water Management Software Mobile Application provided by Assurity Consulting Ltd (including the entity of Assurity Consulting Holdings Ltd) as a part of our contractual agreements. We process personal data where necessary for the performance of our contract with customers, compliance with legal obligations, and our legitimate interests in operating, securing and improving our services.

Topics:

Why do we process your personal data and what information do we collect?

How do we use the information collected?

What data security measures are in place?

Children's privacy

What data will be shared?

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

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 and what information do we collect?

The mobile application is used by authorised personnel to manage water systems within buildings, record inspections, perform specified tasks, maintain asset information and support water management processes as instructed, when using the Assurity Plus 2.0 Water Management Software. We only collect necessary personal data in order to provide required users with relevant access and track user inputs in order for complete records of task completion.

Information we collect:

User Account Information

- User name
- Email address
- User identifier
- Login credentials
- Account permissions and access roles

Site and Asset Information

- Building information

- Site information
- Water system information
- Asset and equipment information
- Compliance records

Operational Records

- Inspection records
- Monitoring records
- Maintenance records
- Corrective action records
- Notes and comments entered by users

Photographs

The application allows users to capture and upload photographs to support:

- Inspections
- Maintenance activities
- Compliance evidence
- Asset identification
- Reporting activities

QR Code Data

The application uses QR codes that are only provided securely for:

- Site identification
- Accessing relevant site records within the system

Device and Technical Information

We may automatically log information including IP address, device identifiers, application events, crash reports and technical diagnostics necessary to maintain security and service performance.

The application may use third-party service providers for hosting, authentication, notification delivery, diagnostics and technical support.

Information We Do Not Collect

The application does not collect or track precise GPS location information.

The application is not designed to collect personal information unrelated to the operation of water management and compliance activities.

Camera and QR Code Usage

The application requires access to the device camera for legitimate business purposes including:

- Capturing inspection photographs
- Recording compliance evidence
- Scanning QR codes used for authentication
- Scanning QR codes used to identify sites

Camera access is used only when initiated by the user. The application requests device permissions only where necessary for operation of the service. Users may manage permissions through device settings.

Images and QR code information are used exclusively to support the operation of the Water Management System.

Push Notifications

The application uses push notifications to provide the user with information, including:

- Inspection reminders
- Scheduled task notifications
- Status alerts
- System messages
- Task updates
- Important service notifications

Push notifications are used solely for operational and service-related purposes and are not used for advertising or marketing.

Users can manage notification preferences through their mobile device settings where supported.

How We Use the Information?

We use information processed through the application to:

- Authenticate authorised users
- To verify management site water services, their assets, chemical and equipment
- Review and share tasks, jobs and other activities recorded for a site
- Generate reports and audit records
- Provide customer support and dashboard information
- Maintain service security and availability
- Investigate technical issues
- Improve application performance and reliability

What data security measures are in place?

Assurity Consulting takes appropriate technical and organisational measures to protect information processed through the mobile application.

Security measures include:

- Encryption of data transmitted over public networks using HTTPS/TLS
- User authentication controls
- Role-based access controls
- System monitoring and logging
- Secure hosting environments
- Regular security updates and maintenance procedures

- Protection against unauthorised access, disclosure, alteration and destruction

While we take all reasonable steps to protect information, no method of electronic transmission or storage can be guaranteed to be completely secure.

Children's privacy

The application is intended for use by authorised personnel in a business environment and is not directed to children under the age of 18. We do not knowingly collect personal information from children.

What data will be shared?

Assurity Consulting will share information only:

- With the organisation subscribing to the Water Management System service
- With authorised service providers supporting delivery of the service
- Where required by law, regulation or legal process
- Where necessary to protect the security, integrity or operation of our services

Any third-party service providers are required to process information in accordance with applicable contractual and legal requirements.

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 Assurity Plus 2.0 Water Management Software Mobile Application the data is collected by our customer who is the data controller or their instructed supplier]
- 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.

What are the lawful bases for processing the data?

Customers

We will only process customer data on the Assurity Plus 2.0 Water Management Software Mobile Application for the fulfillment of a contractual agreement between the customer and Assurity Consulting Ltd.

Former customers

We will not process any personal customer data on the Assurity Plus 2.0 Water Management Software Mobile Application if our contractual agreement has ended. In this case, we will provide you with the data export and access for your company to Assurity Plus will cease after 1 year 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.

Who is the data controller and who processes your data?

Assurity Consulting Ltd acts as a **data controller** for personal data processed in connection with user account administration, service operation, platform security, technical support and related business functions. For operational records, inspection data, compliance records and other information entered into the system by customer organisations and their instructed suppliers, the customer organisation will act as the data controller. In some circumstances Assurity Consulting Ltd and the customer organisation **may act as joint controllers** where both parties jointly determine the purposes and means of processing.

Assurity Consulting employees delivering work as part of our contractual agreement will have access to the data within the application for the purposes of verifying task and job completion and reviewing other records in order to complete their audits as agreed.

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 international transfers of personal data are carried out in accordance with applicable UK data protection legislation and appropriate safeguards including adequacy regulations, standard contractual clauses or equivalent lawful transfer mechanisms.

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 realise and be as specific as possible with what you want so that we can prioritise your request. You can also search the public register on the Information Commissioner'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 – Where applicable, you have the right to receive personal data you have provided in a structured, commonly used and machine-readable format.

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:

Registered Address: Assurity Consulting Ltd 26 Redkiln Way Horsham West
Sussex RH13 5QH United Kingdom

Company registration number: 2227268

Email: dataprotection@assurityconsulting.co.uk

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