# Intellitect Water

## Data Protection Policy

Reference: data Protection
Issue No: 3
Issue Date: 04/07/2022

## 1 Objective / Purpose

This policy outlines key data protection incentives which Intellitect Water Ltd. (IWL) adhere to. The purpose of this document is to provide transparency to our customers before and during our working relationship.

We therefore seek to ensure that IWL:

- Are clear about how personal data must be processed.
- Comply with the data protection law and legislation.
- Protect the company's reputation by ensuring the personal data entrusted to us to processed in accordance with data subjects' rights.
- Protect the company from risk of breaching data protection law.

Updates to this document are periodically added here: www.intellitect-water.co.uk

## 2 Scope

This policy applies to all tenant data collected by IWL.

## 3 Data Protection Principles

Personal Data must be:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness, and transparency).
2. Collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation).
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (Data minimisation).

4. Accurate and where necessary kept up to date (Accuracy).
5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation).
6. Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage (Security, integrity, and confidentiality).

# 4 Policy specifics

## 4.1 Accountability

We understand the importance of getting Data Protection right and commit to the following:

- Nominating a person (suitably qualified) who oversees Data Protection in the organisation.
- Implementing privacy by design and completing Data Protection Impact Assessments whenever there is a change to the processing of personal data.
- Ongoing staff training on data protection.

## 4.2 Responsibilities

### 4.2.1 IWL

As the Data Controller we are responsible to the policies and procedures to comply with data protection law.

### 4.2.2 Staff

Staff members who process personal data on behalf of our customers must comply with the Internal data protection policy. In essence they must ensure that:

- All data is kept securely
- No personal data is disclosed verbally or in writing to any unauthorised third party
- Personal data is kept in accordance with our retention schedule
- Any queries regarding data protection are forwarded on to the appropriate person to deal with. This includes any data subject requests.
- Any breaches of data protection are brought to the appropriate person to raise with the ICO.
- If they are uncertain about anything that they seek advice from the appropriate person in the company.

### 4.2.3 Third Parties

Where external companies are used to process data on behalf of IWL reasonable steps are taken to ensure that they provide adequate security measures to protect the personal data being processed.

## 4.3 Ownership

- All RAW data that is collected from IWL hardware over the course of a partnership between IWL and a customer remains property of the customer.
- All RAW data that is collected from hardware not manufactured by IWL remains property of the customer.

- Some customers buy IWL hardware, some customers rent hardware. Irrespective of device ownership IWL remain owners of all diagnostic data which enables troubleshooting for the life of the hardware.
- IWL may continue to use any data published to their Insight system to aid in statistical analysis only. All personal data and any company identification is removed as standard. The data remaining relates to water, location, and event data.
- Special requests for complete data deletion can be accommodated (fees may apply).

## 4.4 Location of data

- All data that is collected and used on the Insight system is in secure datacentres which are in the UK.
- IWL use a trusted partner who owns and maintains the data centre. A required standard for them is to maintain their ISO27001 compliance.
- Working documents used by the back office are held in a secure data centre on premise within the organisation.
- Office 365 is used for email and thus uses Microsoft Cloud Infrastructure.

## 4.5 Restricted Access

Access to customer data is restricted to employees that need the access to carry out their job.

## 4.6 What we collect and why…

There is currently no requirement for IWL to record any special category data for our customers.

| Record | Location | Reason for recording | Clarification |
|---|---|---|---|
| *Name* | Onsite and Cloud Data Centre | Identification, verifications, communication, system requirement | Normal |
| *Email* | Onsite and Cloud Data Centre | Identification, verifications, communication, system requirement | Normal |
| *Phone Number* | Onsite and Cloud Data Centre | Identification, verifications, communication, system optional requirement | Normal |
| *Company* | Cloud Data Centre | Identification, system requirement | Normal |
| *Department* | Cloud Data Centre | System optional requirement | Normal |
| *Roles* | Cloud Data Centre | System optional requirement | Normal |

| | | | |
|---|---|---|---|
| *IP Address* | Cloud Data Centre | Logging | Normal |
| *User Agent* | Cloud Data Centre | Logging | Normal |
| *Avatar* | Cloud Data Centre | System optional requirement | Normal |

## 4.7 Data Subject Rights

If you would like to exercise your rights as a Data Subject, please email support@intellitect-water.co.uk. These rights include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

# 5 Insight infrastructure

IWL's core program (Insight) is constantly under development both to enhance features and to increase security. Below is a list of key points which have been implemented to ensure a smooth operation and secure environment for our customers.

- We outsource our server requirements to an ISO27001 accredited provider that specialises in operating and constantly available secure data centre.
- A completely scalable environment which is constantly monitored to ensure a responsive user experience.
- Multiple locations providing increased uptime and improved redundancy.
- Regular backups with 7-day retention.
- Security and feature patch management to ensure the environment is kept up to date (once patches have been tested).
- Standard data retention for customers is five years. This is flexible depending on what the customer requires.
- Software upgrades and design is with privacy in mind.
- Firewall setup to industry standards (ports closed, SSH disabled remotely etc.)
- MFA enabled across the platform.

# 6 General IT infrastructure

- Sophos Intercept X has been installed across all Endpoints and Servers.
- Monthly patch management program to ensure all machines are on the latest software.
- Encryption of all hard drives that hold company data.
- Sophos XG Firewall.

- MFA fully enabled across the office tenancy.
- MFA required for VPN access through firewall.
- Fob entry to site.
- CCTV across site.
- Server room is kept locked, and access is restricted.
- Large UPS guarantees system availability.
- Password policies to ensure users properly protect their workstation.
- Auto lock for PCs after 10 mins of inactivity.

# 7 Advertising

We do not currently perform targeted advertising of our current or future services to any of our customers. If this changes then it will be on an 'opt-in' basis in accordance with GDPR and Data Protection Act 2018.

04/07/2022

**Steve Willis CEO** **Intellitect Water Ltd.**