GDPR COMPLIANCE POLICY

Charles Tennant & Co (NI) Ltd
Charles Tennant & Co (Cork) Ltd
Tennants Building Products Ltd
Walls & Ceilings International Ltd

Introduction

Charles Tennant & Co (NI) Ltd, Tennants Building Products Ltd, Charles Tennant & Co (Cork) Ltd, and Walls & Ceilings International Ltd (Tennants) have a comprehensive GDPR Compliance Programme across all areas of the business where personal data is held and processed. A full information audit has been carried out and new policies and procedures have been put in place to form our GDPR Policy, which is designed to ensure that we meet our new accountability obligations, as well as all other new or updated requirements.

The programme is overseen by our Data Protection Officers, Catherine Simmons (Tennants) and Julian Workman (Walls & Ceilings) and the Data Protection Steering Committee.

Data Protection Act 1998

The Data Protection Act controls how personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- Used fairly and lawfully.
- Used for limited, specifically stated purposes.
- Used in a way that is adequate, relevant and not excessive.
- Accurate.
- Kept for no longer than is absolutely necessary.
- Handled according to people's data protection rights.
- Kept safe and secure.
- Not transferred outside the European Economic Area without adequate protection.

The General Data Protection Regulation (GDPR)

GDPR has adopted the same basic principles as the data protection law however they have been strengthened with more accountability and higher penalties.
The key features of the GDPR include:

- Enhanced rights for individuals – including the right to object to certain types of profiling and automated decision making.
- Obligations on organisations to publish more detailed fair processing notices – informing individuals of their data protection rights, how their information is being used and for how long.
- Stringent consent requirements – consent must be explicit and freely given for a specific purpose, and must be easy to retract.
- Data processors – new requirements are imposed on data processors, including elements which should be addressed contractually between them and data controllers.
- Breach reporting – significant data breaches must be reported to regulators within 72 hours
- Privacy impact assessments – organisations must formally identify emerging privacy risks, particularly those associated with new projects
- Privacy by design – organisations must design data protection into new business processes and systems
- Record keeping – organisations must maintain registers of the processing activities that are carried out

Formal training has been completed with all Tennants employees who access and / or process personal data.

Data Subjects & Consent

Employee data and consent to the obtaining, retaining and processing of that data is governed by our Employee Privacy Notice which is incorporated into the Tennants Employee Handbook.

Customer data is obtained, retained and processed for business purposes only and consent to the obtaining, retaining and processing of that data is given via the Tennants Credit Application Form, which is completed at the outset of the business relationship.

Supplier data is obtained, retained and processed for business purposes only and consent to the obtaining, retaining and processing of that data is implicit in our trading relationship.

At the commencement of our compliance programme all existing data subjects were notified of our GDPR Policy.

We are aware that images recorded via our CCTV systems constitute personal data and such images and consent for same are governed by our CCTV Policy.

Disclosure and Sharing of Personal Data

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

Data Subject Management

All individuals are allowed to access their personal data to be aware of the information held, to verify the lawfulness of the processing of their data and they have the right to rectify or erase any data they believe to inaccurate or incomplete. The individual can access the information via a Subject Access Request (SAR) submitted to the Data Protection Officer.

The Steering Committee will meet to discuss the validity of the request and report to the individual within one month where possible. Where this data has been shared with a third-party, we will inform the third-party of the request.

Third-Party Processors / Accessors

A third-party data processor is an entity that processes personally identifiable information on our behalf or has access to such information. Any third-party processor or accessor that we use is now directly and legally obligated to also be in compliance with GDPR.

A GDPR Register of all Tennants third-party processors and accessors has been compiled and all have been assessed for compliance with GDPR and are aware of their obligations. Any new third-party processors or accessors introduced will be assessed in the same way.

Data Breaches

Where relevant it is the responsibility of the Data Controller and Data Processor to jointly report any breach or suspected breach within 72 hours of the incident to the ICO. A breach is defined as a loss or potential loss of personal data.

Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his office.

The nature of the breach or loss can then be considered, together with whether the Data Controller is properly meeting his responsibilities under the GDPR.

'Serious breaches' are not defined. However, the information at ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf should assist data controllers in considering whether breaches should be reported.

Privacy Impact Assessments (PIA)

Privacy Impact Assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. The aim of PIAs is to minimise personal information risk and an effective PIA will allow us to identify and fix problems at an early stage

In view of this, any changes to processes, or new processes or projects added to our systems will consider privacy where applicable. A member of the steering committee will perform a PIA during any applicable projects and all such projects will be designed to minimise the amount of personal data held.

Related Policies

The following policies are linked to our overall GDPR Compliance Programme and are available on request.

- Employee Privacy Notice
- Document Retention
- Hard Copy Security
- CCTV
- Customer Card Payments
- Network Security

Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.