

## Introduction

The EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), and the Data Protection Act 2018 (DPA 2018) came into force on 25 May 2018, superseding the Data Protection Act 1998. GDPR will continue to apply despite Brexit and impacts all organisations that control or process personal data.

Following the Brexit transition period, the DPPEC (The Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019 combined the EU GDPR's provisions with the DPA 2018's "applied GDPR" to form a UK data processing regime called the "UK GDPR", which has applied in the UK since 1 January 2021.

UK organisations that process personal data must therefore comply with:

- The DPA 2018 and UK GDPR if they process only domestic personal data.
- The DPA 2018 and UK GDPR, and the EU GDPR if they process the personal data of UK residents and offers goods and services to, or monitor the behaviour of, EU residents.

Where so required LRL Roofing Solutions will comply with the provisions of both EU GDPR and UK GDPR. Transfers of information to and from the European Economic Area (EEA) will be in line with both the UK GDPR and EU GDPR. The abovementioned Act and Regulation grants data subjects a range of new rights, giving them more control over how their data is used. Organisations are subject to new responsibilities and obligations, including the need to demonstrate compliance.

**We also include within this policy the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.**

This policy applies to current, future and former clients. We are a Data Controller of the personal data that you supply to us under your contract with us.

## Data Protection Principles

Under UK GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

1. processing is fair, lawful and transparent
2. data is collected for specific, explicit, and legitimate / lawful purposes
3. data collected is adequate, relevant and limited to what is necessary for the purposes of processing
4. data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
5. data is not kept for longer than is necessary for its given purpose
6. personal data will be kept secure
7. data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
8. personal data is not transferred to countries outside of the European Economic Area (EEA) without adequate protection.

## **Commitment**

We are committed to the principles inherent in the UK GDPR and particularly to the concepts of privacy by design, the right to be forgotten, consent and a risk-based approach. In addition, we aim to ensure:

1. transparency with regard to the use of data
2. that any processing is lawful, fair, transparent and necessary for a specific purpose
3. that data is accurate, kept up to date and removed when no longer necessary
4. that data is kept safely and securely.

## **Policy**

This data protection policy is available on our website and a copy will be made available to all employees and to clients, contractors and suppliers associated with this organisation by issuing an electronic copy or by sign posting them to the link on our website. It will be updated if the legislation changes or further guidance is available.

## **Types of Data Held**

We keep several categories of personal data on and from our clients in order to carry out effective and efficient processes. We hold the data within our computer systems, for example, the systems that we use to provide our services.

Specifically, we hold the following types of data:

1. personal details such as name, address, phone numbers, job title, email addresses etc for the main contact and other contacts for the delivery of the service
2. personal details such as name, address, phone numbers, job title / trade, email addresses, job description, salary, disciplinary and grievance records, annual leave records, criminal convictions, sickness, accident and incident data, family related leave, appraisal, performance information, etc provided to us for the delivery of the service
3. gender, marital status, race, religion, trade union membership, information of any disability that employees may have or other medical information that is supplied to us for the purposes of delivering the service (advice, litigation etc)
4. bank account details
5. invoice address and invoice activity
6. IT service use including online service access records.

## **Collecting Your Data**

You provide several pieces of data to us directly when enquiring about our services, including meetings, when the service agreement or contract is signed, during the delivery of our services and after the contract / service provision has ended. Personal data is kept in files or within the Company's IT systems.

## **Lawful Basis for Processing**

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data in order to comply with a legal requirement or in order to effectively manage the service contract we have with you, including ensuring we can deliver the service to you.

The information below categorises the types of data processing we undertake and the lawful basis we rely on.

Activity requiring your data	Lawful basis
Set up your account	Performance of services / contract
Carry out the delivery of our services	Performance of services / contract
Ensuring payments are made under your account	Performance of services / contract
Ensuring VAT and insurance premium tax is paid	Legal obligation
Carrying out checks in relation to your company status and validating the information supplied to us	Legal obligation
Making financial decisions in relation to entering both initial and subsequent contracts	Our legitimate interests
Making decisions about service delivery methods	Our legitimate interests
Ensuring efficient administration of contractual services to you	Our legitimate interests
Effectively monitoring the service provided including adherence to commitments and service entitlements	Our legitimate interests
Maintaining up to date records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in place	Our legitimate interests
Dealing with legal claims made against us	Our legitimate interests
Preventing fraud	Our legitimate interests
Ensuring our administrative and IT systems are secure and robust against unauthorised access	Our legitimate interests

## Special Categories of Data

Special categories of data are data relating to:

1. health
2. sex life
3. sexual orientation
4. race
5. ethnic origin
6. political opinion
7. religion
8. trade union membership
9. genetic and biometric data.

We carry out processing activities using special category data for the purposes of delivering advisory services in relation to employment and health and safety legislation. This data will be provided to us or requested by us for the purposes of providing our services, to ensure you receive appropriate advice and support.

Most commonly, we will process special categories of data when the following applies:

1. you have given explicit consent to the processing
2. we must process the data in order to carry out our legal obligations
3. we must process data for reasons of substantial public interest
4. you have already made the data public.

## **Failure to Provide Data**

Your failure to provide us with relevant data may mean that we are unable to fulfil our requirements for entering into a contract with you. This could include being unable to offer you services or administer existing contractual services.

## **Criminal Conviction Data**

We will only collect criminal conviction data where it is appropriate to the provision of the services that you are contracted to receive. This data will usually be collected at the advisory stage or the litigation stage, however, it may be collected at any time during the contract where necessary. We use criminal conviction data to manage potential or future litigation from client employees and workers. We use the information to form the advice and services that are provided to clients. We rely on the lawful basis of legitimate interest to process this data.

## **Who We Share Your Data With**

All employees within the company that handle your personal data are trained in ensuring data is processed in line with UK GDPR and the DPA 2018.

Your data is not shared with third parties, except for other reasons to comply with a legal obligation placed upon us.

## **Protecting Your Data**

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

## **Retention Periods**

We only keep your data for as long as we need it for, which will be at least for the duration of your service contract plus 7 years from the date that service contract with us terminates, although in some cases we will keep your data for a longer period after your contract has ended. Some data retention periods are set by the law.

Retention periods can vary depending on why we need your data, as set out below:

Record	Recommended Retention Period
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently
HMRC approvals	Permanently
Money purchase details	6 years after transfer or value taken
Health data	30 or 50 years
Litigation cases	7 years from the conclusion of the litigation case
All other data	7 years from the date the service contract with us terminates

## Automated Decision Making

Automated decision-making means making decision about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

## Client Rights

You have the following rights in relation to the personal data we hold on you:

1. the right to be informed about the data we hold on you and what we do with it
2. the right of access to the data we hold on you
3. the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification'
4. the right to have data deleted in certain circumstances. This is also known as 'erasure'
5. the right to restrict the processing of the data
6. the right to transfer the data we hold on you to another party. This is also known as 'portability'
7. the right to object to the inclusion of any information
8. the right to regulate any automated decision-making and profiling of personal data.

## Right to Be Forgotten

We recognise the right to erasure, also known as the right to be forgotten, laid down in the UK GDPR. Individuals should contact Head office with requests for the deletion or removal of personal data. These will be acted on provided there is no compelling reason for continued processing and that the exemptions set out in the UK GDPR do not apply. These exemptions include where the personal data is processed for the exercise or defence of legal claims and to comply with a legal obligation for the performance of a public interest task or exercise of official authority.

## Subject Access Requests

We recognise that individuals have the right to access their personal data and supplementary information and will comply with the one-month timeframe for responses set down in the UK GDPR. As a general rule, a copy of the requested information will be provided free of charge, although we reserve the right to charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive. If this proves necessary, the data subject will be informed of their right to contest our decision with the supervisory authority (the Information Commissioner's Office (ICO)) whose contact details are set out below.

As set out in the UK GDPR, any fee will be notified in advance and will be based on the administrative cost of providing the information.

## Children

The UK GDPR provides for special protection for children's personal data and we will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16.

## Consent

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

## Data Loss

If a data breach occurs that is likely to result in a risk to the rights and freedoms of individuals, the people affected will be informed as soon as possible and the ICO will be notified within 72 hours.

## Making a Complaint

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>

This Policy will be reviewed no later than 12 months from the date below.

Signed for and on behalf of LRL Roofing Solutions



Mr. Robert Richmond

**Designation:** Managing Director

**Date:** 27<sup>th</sup> November 2022