# Company Data Protection Policy

## *Direct Data Analysis*

Data Protection Registration Number: Z3022378

This document is to be read by all persons employed, who also need to sign that they have read and fully understand the data protection policy of Direct Data Analysis.

*Updated June 2026 – Version 4*

June 2026

# Data Protection Policy

## Introduction

The Data Protection Act 2018 (DPA) and the UK GDPR set out the legal requirements and duties placed on data controllers (the Client), and data processors (anyone the Client uses to process data on their behalf), and explain the 'information rights' held by data subjects (people we hold information about).

The policy will inform you how the UK GDPR applies to Direct Data Analysis and our obligations.

Direct Data Analysis (The Company) is required to collect and store certain personal data as part of its business activities. The Company recognises the importance of the correct and lawful treatment of personal data; it maintains confidence in the organisation and provides for successful operations.

The types of personal data that the Company may require include information about members of the public and company employees who have given permission for data to be collected for survey research and analysis purposes. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Company fully endorses and adheres to the UK GDPR principles. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for the Company must adhere to these principles.

Any person working with data for or on behalf of Direct Data Analysis needs to be aware of this policy and confirm by signature that they fully understand and will always abide by the policy.

### Principles

The UK GDPR requires that personal data shall:

1. Be processed lawfully, fairly and transparently;
2. Be collected for specified, explicit and legitimate purposes;
3. Be adequate, relevant and limited to what is necessary;
4. Be accurate and, where necessary, kept up to date;
5. Not be kept for longer than is necessary for the purposes for which it is processed;
6. Be 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 and organisational measures.

Personal data must not be transferred outside the UK unless appropriate safeguards are in place, such as an adequacy regulation, the International Data Transfer Agreement (IDTA), or the UK Addendum to the EU Standard Contractual Clauses.

## Satisfaction of principles

In order to meet the requirements of the principles, the Company will:

- observe fully the conditions regarding the fair and lawful collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or legal requirements;
- ensure the accuracy and quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held can be fully exercised under the UK GDPR and the Data Protection Act 2018;
- take the appropriate technical and organisational security measures to safeguard personal data;
- and ensure that personal data is not transferred outside the UK without appropriate safeguards.

## The Company's Designated Data Controller

The Company Data Controller is responsible for ensuring compliance with the UK GDPR and the Data Protection Act 2018, and for overseeing the implementation of this policy on behalf of the Company. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Company Data Controller.

## Status of the Policy

Any employee who considers that the policy has not been followed in respect of personal data should raise the matter with the Company Data Controller in the first instance.

Any breach will be taken seriously and may result in formal action.

## Subject Access

All individuals have the right to request access to their personal data under the UK GDPR. Requests must be made in writing to the Company Data Controller. The Company will respond within one month of receipt. This may be extended by a further two months for complex requests, in which case the individual will be informed. No fee will be charged unless the request is manifestly unfounded or excessive. Identity verification may be required before information is released.

## Employee Responsibilities

All employees are responsible for:

- Checking that any personal data that is provided to the Company is accurate and up to date.
- Ensuring that any change to information which has been provided, e.g. changes of address, is processed swiftly and accurately.
- Checking any information that the Company may send out from time to time, giving details of information that is being kept and processed.

- If, as part of their responsibilities, employees collect information about other people (e.g. about personal circumstances), they must comply with the Policy and with the Data Protection Procedures which are contained in the Data Protection Manual.

### Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely at all times.
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.
- Computer screens are locked to prevent unauthorised viewing when the authorised user is away from the computer.
- No personal data is to be viewed or worked upon in a public area (i.e. on the train).
- Homeworking is only allowed following a) Reading and signing of the Company 'Teleworking and mobile working procedures' document, and b) Completion of the 'Request for mobile working' form and c) Security procedures signed off by our IT lead.
- Data is not allowed to be stored on employees' own personal computers.

### Data will be secured in two levels as follows:

- All devices that hold data (computer, laptop, portable data storage device) are password protected to prevent unauthorised access.
- Databases, spreadsheets and all other data storage programmes to be password protected. This must be a separate password to that required to access the computer/storage device.
- All passwords must be a minimum of 12 characters. Password complexity rules are not required, but passwords must be strong and unique. Passwords must not be reused across systems.

### Rights to Access Information

All individuals have the right to request access to their personal data under the UK GDPR. Requests must be made in writing to the Company Data Controller. The Company will respond within one month of receipt. This may be extended by a further two months for complex requests, in which case the individual will be informed. No fee will be charged unless the request is manifestly unfounded or excessive. Identity verification may be required before information is released.

### Subject Consent

The purpose to collect and process data should be communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race or gender, then where a person may be identified from the data stored, express consent to process the data must be obtained.

### Retention of Data

The Company will retain personal data only for as long as necessary for the purposes for which it was collected, in accordance with agreed retention schedules and the principles of the UK GDPR. Personal

data must not be kept for longer than required, and retention periods must be reviewed regularly to ensure ongoing compliance.

When data is no longer required, it must be securely erased using approved disposal methods:

### Paper Data:

- Must be cross-cut shredded or placed in secure confidential-waste disposal.
- Disposal must be carried out by authorised staff or an approved secure-destruction provider.
- No paper records containing personal data should be placed in general waste or recycling.

### Electronic Data:

- Must be deleted using approved secure-deletion methods that prevent recovery.
- Portable media (USB drives, temporary storage devices) must be securely wiped and reformatted before reuse or disposal.
- Company computers and laptops must have data removed using the approved secure-erase or “data cleaner” tools installed by the IT Lead.
- No personal data may be stored on company devices.

### Breach of Data Protection and Confidentiality

All data protection incidents or suspected breaches must be reported immediately to the Company Data Controller. Where a breach presents a risk to individuals’ rights and freedoms, the Company will assess the incident and, if required, report it to the Information Commissioner’s Office (ICO) within 72 hours. Individuals affected by a high-risk breach may also be notified where required.

### Employee Understanding of the Policy

I [insert name of employee here] confirm that I have read, understand, and will comply at all times with this Data Protection Policy issued by Direct Data Analysis, and that any breach of the policy may lead to disciplinary action or dismissal from employment.

Signed: ……

Print Name: ……

Date: ……..