

Result Clothing Ltd Data protection policy

This document sets out the policy and principles adopted by Result Clothing Ltd (hereinafter '**Result**') for the processing and security of personal data.

Context and overview

Key details

- Policy reviewed by: K Brown
- Approved by board / management on: 1st May 2018
- Policy became operational on: 1st May 2018.
- Last review date: 9th September 2025
- Next review date: 9th September 2027

Introduction

Result needs to gather and use certain information about individuals. This can include customers, suppliers, business contacts, employees and other people the organisations have a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures that **Result**

- Comply with data protection law and follow good practice
- Protect the rights of staff, customers and partners
- Are open about how they store and process individuals' data
- Protect themselves from the risks of a data breach

Data protection law

GDPR legislation describes how organisations — including **Result** must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR legislation is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary

6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of **Result**
- All staff and volunteers of **Result**
- All contractors, suppliers and other people working on behalf of **Result**

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ...plus any other information relating to individuals

Data protection risks

This policy helps to protect **Result** from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with **Result** has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **board of directors** is ultimately responsible for ensuring that **Result** meet their legal obligations.

The **IT manager, K. Brown**, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

The **Marketing Managers, S Sanders-Smith** are responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- **Result** will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, for example: on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to **Result** unless the businesses can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Always access and update the central copy of any data.

Data accuracy

The law requires **Result** to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort **Result** should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- **Result** will make it easy for data subjects to update the information the companies hold about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

CCTV

Footage recorded on our security systems is also part of GDPR guidelines, therefore steps must be taken to ensure privacy of employees and visitors is protected.

- Signage must be clearly visible in all buildings where CCTV is in operation to advise public and employees that they may be recorded.
- Access to CCTV recordings is controlled; recordings can only be accessed via the IT manager. Live footage can be accessed by directors and warehouse managers.
- Recordings are stored on password secured hard disk recorder located in (comms room in Beccles and managers office in Colchester).
- CCTV is installed primarily for security purposes, it is there to deter theft, and in event of a break in would allow police to hopefully identify culprits. It may also be used for other safety and disciplinary matters.
- CCTV only covers workplace areas, building perimeters and warehouse, it is not installed in canteens, toilets or other areas where employees would expect privacy.
- Approx. 1 month of footage is stored on the hard drives at any time, it is automatically overwritten by the CCTV system.
- Footage is available to be viewed on request at any time by contacting the IT Manager, so long within 1 month recording window.
- Audio is recorded on certain newer warehouse cameras as useful in event of a break in.

Employee Data

Please refer to the privacy notice for employees and workers in the company handbook for details.

Subject access requests

All individuals who are the subject of personal data held by **Result** are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the IT Manager. The IT Manager can supply a standard request form, although individuals do not have to use this. We will normally comply with your request at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may contact you requesting a fee. The IT Manager will aim to provide the relevant data within 30 days. But where requests are complex or numerous, we may contact you to inform you that timeframe

may be extended. The IT Manager will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the GDPR legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, **Result** will disclose requested data. However, the IT Manager will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Result aim to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the companies have a privacy statement, setting out how data relating to individuals is used by them. This is available on request. A version of this statement is also available on the company's website.