

Data Protection Policy

TST IMPRESO needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees, and other people the organization has 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.

This data protection policy ensures TST IMPRESO:

Complies with data protection law and follow good practice

Protects the rights of staff, customers and partners

Is open about how it stores and processes individuals' data

Protects itself from the risks of a data breach

Policy scope

This policy applies to:

The head office of TST IMPRESO

All branches of TST IMPRESO

All staff and volunteers of TST IMPRESO

All contractors, suppliers and other people working on behalf of TST IMPRESO

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. 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 TST IMPRESO 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 TST IMPRESO 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.

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.

TST IMPRESO 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 unauthorized 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 protection officer 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 or data controller. When data is stored on paper, it should be kept in a secure place where unauthorized 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 unauthorized people could see them, like 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 unauthorized 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.

Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

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 TST IMPRESO unless the business 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 authorized external contacts.

Personal data should never be transferred outside of the US Economic Area.

Employees should not save copies of personal data to their own computers.

Always access and update the central copy of any data.

Data accuracy

The law requires TST IMPRESO 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 TST IMPRESO 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.

TST IMPRESO will make it easy for data subjects to update the information TST IMPRESO holds about them.

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.

Subject access requests

All individuals who are the subject of personal data held by TST IMPRESO 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 data controller at [1].

The data controller 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 Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, TST IMPRESO will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

TST IMPRESO aims 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 company has a privacy statement, setting out how data relating to individuals is used by the company.

purposes under any circumstances.

All the above categories of personal data collected by TST/Impreso, Inc. exclude text messaging opt-in data. This information is kept entirely confidential and is only used to communicate directly with you in accordance with your explicit consent.