Data Security and Protection Procedure

Document Control Sheet

Revision	Date	Description of changes/amendments	Prepared by	Approved by
00	16/5/18	New procedure created	R Fleming	R Fleming

Contents

1. Introduction

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

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

For the purposes of this procedure 'Staff' will refer to all employees of TLI Group and all individuals subcontracted into complete works on behalf of TLI Group.

2. Purpose

This data protection procedure ensures TLI Group:

- Complies with data protection law and follow good practice;
- Protects the rights of staff, customers and partners;
- Will clearly state how it stores and processes individuals' data;
- Protects all data on file from the risks of a data breach.

3. Data protection law

The General Data Protection Regulation 2016/679 describes how TLI Group — will collect, handle and store personal information.

These regulations apply regardless of whether data is stored electronically, on paper or in other formats.

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

The General Data Protection Regulation is underpinned by eight important principles.

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.

4. Procedure scope

This procedure applies to:

- TLI Group and TLI Group UK;
- All divisions of TLI Group;
- All staff of TLI Group;
- All subcontractors, suppliers and other people working on behalf of TLI Group.

This procedure applies to all data TLI Group holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 2016/679. This can include:

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

5. Data protection risks

This procedure helps to protect TLI Group from some very real data security risks, including but not limited to:

- **Breaches of confidentiality.** E.g. Information being given out inappropriately;
- **Failing to offer choice.** E.g. All staff should be free to choose how the company uses data relating to them;
- **Reputational damage.** E.g. TLI Group could suffer if hackers successfully gained access to sensitive data.

6. Responsibilities

TLI Group staff are responsible 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 procedure and data protection principles.

However, the staff has key areas of responsibilities:

- The **Board of Directors** is ultimately responsible for ensuring TLI Group meets it's legal obligations.
- The **Data Protection Officer, Russell Fleming**, is responsible for:
    - Keeping the board updated about the data protection responsibilities, risk and issues;
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule;
    - Arranging data protection training and advice for the people covered within this procedure;
    - Handling data protection questions from staff and anyone else covered within this procedure;
    - Dealing with requests from staff to see the data TLI Group holds about them (also called 'subject access requests');
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data;
    - 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.

- The **IT Manager,** 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 third-party services, TLI Group uses to store or process data. E.g cloud computing services.

- The **Business Development Director,** is responsible for:
    - Where necessary, working with staff to ensure marketing initiatives abide by data protection principles.

7. General staff guidelines

- People able to access data covered by this procedure should be those who **require it for their work;**
- Data **should not be shared informally.** When access to confidential information is required, staff must request if from their line managers and/or the data protection officer;
- **TLI Group will provide training** to all employees to help them understand their responsibilities when handling data;

Staff should keep all data secure, by taking sensible precautions and following the guidelines bellows.

- **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 and/or no longer required, it should be deleted and disposed of. E.g. shredded.
- Employees **should request assistance** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

8. Data storage

These rules outline 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 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 / filing cabinet;**
- Staff should make sure paper and printouts are **not left where unauthorised people could see them**;
- **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 password**s that are changed regularly and never shared between employees;
- Data **stored on removable media** (link USB Key or DVD), 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 **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.**

9. Data use

Personal data is of no value to TLI Group 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 authorised external contacts.
- Personal data should never be **transferred outside of the European Economic Area.**
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

10. Data accuracy

TLI Group are required under legisation to ensure data is kept accurate and up to date.

It is the responsibility of all staff 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.**
- TLI Group will make it **easy for data subjects to update the information** TLI Group 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.

11. Subject access requests

All individuals who are the subject of personal data held by TLI Group 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 russell.fleming@tli.ie. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

12. Providing information

TLI Group aims to ensure that staff 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.