Data Protection & Privacy Policy

1. Purpose

Threepwood Consulting Ltd (TCL) needs to gather and use certain information about individuals and companies. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

Threepwood Consulting predominantly operate on a 'business to business' basis. As such our policy is not to specifically request personal information from individuals in our client or supplier organisations, except where these individuals are self-employed.

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

If you have any questions about our data protection and privacy policy or any concerns about how we handle and use your personal information then please email info@threepwoodconsulting.com.

This policy ensures TCL:

- Complies with data protection law and follows 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
- Handles and uses personal information for legitimate interests

The Data Protection Act 2018 describes how organisations — including TCL— must collect, handle and store information. The General Data Protection Regulations (GDPR) require us to be transparent about personal information we handle and use.

These rules apply regardless of whether data is stored electronically, on paper or on other mediums.

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

This policy is underpinned by eight important principles, where 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

2. Scope

This policy applies to:

- All offices of TCL
- All staff and agents of TCL
- All contractors, suppliers and other people working on behalf of TCL

It applies to all data that the company holds relating to identifiable individuals or companies, even if that information technically falls outside of the Data Protection Act 2018 and the GDPR. This can include:

- Names, addresses and other contact details provided by individuals:
    - in emails/correspondence sent to us.
    - at conference/workshop/training events we host/attend.
    - through forms on our website.
- Names, addresses, contact details and bank details we request from Associate Consultants or other individuals, who carry out work for us.
- Bank details of individuals who need to pay us for attending our conferences and workshops.
- Personal information in CVs or certifications provided by Associate Consultants (current and prospective) and job applicants.

3. References

TCL Admin Instruction 003

4. Terms and Definitions

Company	Threepwood Consulting Ltd (TCL)

GDPR General Data Protection Regulations

5. Introduction

5.1 Overview

This policy will be implemented to:

- Protect TCL from data security risks, including:
    - Breaches of confidentiality. For instance, information being given out inappropriately
    - Failing to offer choice. For instance, all individuals or companies should be free to choose how the company uses data relating to them
    - Reputational damage. For instance, the company could suffer through unauthorised access to sensitive data
- Comply with the our responsibilities under the GDPR in relation to handling and protecting personal information.

5.2 Responsibilities

Everyone who works for or with TCL will be responsible for ensuring data is collected, stored and handled appropriately.

Each team member that handles data must ensure that it is handled and processed in line with this policy and data protection principles. The following people will have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that TCL meets its legal obligations
- The Business Manager is responsible for:
    - Keeping the board updated about data protection responsibilities, risks 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 by this policy
    - Handling data protection questions from staff, individuals and anyone else covered by this policy

- Dealing with requests from individuals or companies to see the data TCL 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
- 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
- Correcting or removing personal information held about an individual when specifically requested by that individual

- The Managing Director, is 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

6. Guidelines

6.1 General

- 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 the board of directors
- TCL 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 (see Admin Instruction 003)
- 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 the Business Manager if they are unsure about any aspect of data protection or privacy of information

6.2 Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Business Manager.

What personal information do we collect?

- Names, addresses and other contact details provided by individuals:
    - in emails/correspondence sent to us.
    - at conference/workshop/training events we host/attend.
    - through forms on our website.
- Names, addresses, contact details and bank details we request from Associate Consultants or other individuals, who carry out work for us.
- Bank details of individuals who need to pay us for attending our conferences and workshops.
- Personal information in CVs or certifications provided by Associate Consultants (current and prospective) and job applicants.

Where do we store personal data and how do we secure it?

- Any personal information sent by email could be stored on our email server which is only accessible to our staff and is password protected.
- Personal data from suppliers could be stored on our cloud-based customer management system for contacting individuals, raising purchase orders and recording payment of invoices. This system is only accessible to our staff and is password protected.
- Personal information provided in forms, CVs, Service Contracts or other electronic format may be stored on our cloud based file storage system. Areas of this system used for storing personal information are encrypted and only accessible to our staff. This information resides on the hard drives of computers owned by Threepwood Consulting, which are password protected.
- We will store any personal information about individuals we hold as long as we need this to legitimately conduct our business or an individual requests that their personal information is removed.

When data is stored on paper, it shall 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 no longer required, the paper or files shall be shredded and disposed of
- Employees should ensure paper and printouts are not left where unauthorised people could see them

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious access 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, DVD or removable hard drive), these should be kept locked away securely when not being used
- Data should only be stored on designated drives, and should only be uploaded to an approved cloud computing service
- 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

6.3 Data Use

What do we use personal information for?

- Payment to our Associate Consultants and suppliers
- Correspondence and direct communication with individuals in relation to the legitimate conduct of our business
- Circulation of newsletters and similar information to individuals concerning our business activities and consultancy services that they may be interested in

Who do we share personal information with?

- We do not provide personal information we hold on an individual to other third-parties without the express permission of that individual
- We may share personal information provided in CVs by individuals to clients or prospective clients, where that individual is proposed for consultancy services by Threepwood Consulting

What marketing information do we send?

- We only send individuals marketing related correspondence where this is legitimate and in the interest of the individual receiving the correspondence. Individuals may opt out of marketing correspondence by contacting us (see the details provided in Section 1 of this policy)

Personal or company data is of no value to TCL 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 or customer data, employees should ensure the screens of their computers are always locked when left unattended
- Personal or customer data should not be shared informally. In particular, it should never be sent by email unless encrypted, as this form of communication is not secure
- Data must be encrypted before being transferred electronically. The Business Manager can explain how to send data to authorised external contacts.
- Personal or customer data should never be transferred outside of the European Economic Area. This will include data on laptop computers
- Employees should not save copies of personal or customer data to the local storage on their own computers. Always access and update the central copy of any data

6.4 Data Accuracy

The law requires TCL to take reasonable steps to ensure data is kept accurate and up to date

The more important it is that the personal or customer data is accurate, the greater the effort TCL 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 or duplicate data sets
- Staff should take every opportunity to ensure data is up to date. For instance, by confirming a customer's details when they call
- TCL will make it easy for data subjects to update the information TCL holds 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

6.5 Subject Access Requests & Contact Information

All individuals or companies who are the subject of personal or customer data held by TCL 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 deemed a subject access request.

Subject access requests from individuals should be made by email, addressed to the Business Manager at michelle.chambers@threepwoodconsulting.com . The Business Manager can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged. The nominated data controller will aim to provide the relevant data within 14 days.

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

An individual may object to the way we use their personal data or ask us to stop using or to remove personal information we hold about them by contacting us (see our contact details). We will remove this personal information as soon as reasonably practicable and provide confirmation to the individual when this is done.

6.6 Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act and GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

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

Issued by:

Iain Ross
Executive Director

Document History

Version	Date	Amendment	Issued by	Authorised by
1	10/08/16	First issue	Iain Ross Executive Director	Gary Eastwood Managing Director
2	24/05/18	Revised in light of the General Data Protection Regulations (GDPR), that come into effect on 25th May 2018.	Iain Ross Executive Director	Gary Eastwood Managing Director