White & Company PLC

Data Protection Policy

(Revision 1.5)

Revision History

REVISION	DATE OPERATIONAL	CEO/BOARD APPROVAL	NEXT REVIEW	NAME	DESCRIPTION
1.0	01/07/2017	01/07/2017	08/2018	Mr S. Shahi	Original draft
1.1	04/06/2018	03/06/2018	08/2019	Mr M. Corr	Updated to meet changes to Data Protection law
1.2	07/08/2020	07/08/2020	08/2021	Mr. M. Corr	Minor spelling corrections, changes to wording. No Substantial change.
1.3	07/02/2022	07/02/2022	02/2023	Mr. S. Shahi	Updated to UK GDPR
1.4	01/08/2023	01/08/2023	08/2024	Mr. S. Shahi	Minor Changes.
1.5	01/09/2024	01/09/2024	09/2025	Mr. S. Shahi	Minor Changes.

Context and Overview

Introduction

Data Protection law applies to the processing of personal data. The purpose of this policy is to ensure compliance with the UK General Data Protection Regulation - 2021, law that is enshrined by the Data Protection Act 2018 (DPA 2018).

As a company which operates in the European Economic Area we also ensure compliance with the EU GDPR as the provisions of the EU GDPR have been incorporated directly into the UK GDPR. As of 2021, the UK and EEA have operated an adequacy agreement regards the flow of personal data.

White & Company PLC ("White & Co") need to process personal data. 'Processing', in this context, means collecting, storing, using and erasing personal data, irrespective of its format.

Why this policy exists

White & Co processes the personal data of its customers, employees and third-parties. This policy, and staff adherence to it, will ensure White & Co complies with Data Protection law and, in so doing, adopt good practice.

The policy also aims to protect the rights afforded to data subjects by Data Protection law and, together with the Data Privacy Statement, helps to demonstrate White & Co's legal compliance.

Adherence to this policy will protect White & Co from the risks of non-compliance. This includes but is not limited to:

- **Breaches of confidentiality**. For example, information being given out inappropriately.

- **Failing to offer choice**. For example, not informing all customers of their rights over their data which we hold.

- **Reputational damage**. For example, the company could suffer if hackers successfully gained access to company-held personal data.

Data protection law

White & Co is committed to complying with Data Protection law as part of everyday working practices. Complying with Data Protection law can be summarised as but is not limited to:

- Understanding, and applying as necessary, the data protection principles when processing personal data;

- Understanding, and fulfilling as necessary, the rights given to data subjects under Data Protection law; and

- Understanding, and fulfilling as necessary, White & Co accountability obligations under Data Protection law.

As noted, Data Protection law is underpinned by certain principles which govern the processing of personal data. These are:

1. Lawfulness, fairness and transparency.
2. Purpose limitation.
3. Data minimisation.
4. Accuracy.
5. Storage limitation.
6. Integrity and confidentiality (security)

White & Co needs to comply with these six principles and also be able to demonstrate compliance. This requirement to demonstrate compliance is called "accountability" and is a key element of Data Protection law.

People, risks and responsibility

Policy scope

This policy applies to all employees of White & Co (as 'Data Controller') and their processing of company-held personal data.

If another organisation is engaged as a Data Processor, then at White & Co's (as 'Data Controller') request, a Data Processing/Sharing Agreement will be put in place to ensure standards of data protection over company-held personal data are not undermined when shared with third-parties.

Responsibilities

White & Co has a corporate responsibility as a Data Controller (or when acting as a Joint Data Controller or a Data Processor) for:

- Complying with Data Protection law and holding records demonstrating this.

- Cooperating with the Information Commissioner's Office (ICO) as the UK regulator of Data Protection law.

- Responding to regulatory/court action and paying monetary penalties issued by the ICO.

All staff at White & Co share in the collective responsibility for ensuring personal data is collected, stored and used appropriately. However, the following have key areas of responsibility:

The **Board of Directors** is ultimately responsible for ensuring that White & Co meets its legal obligations.

The **Group IT Manager** is responsible for:

- Ensuring all systems, services and equipment used for storing personal 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 example, cloud computing services.

The **Branch Manager** is responsible for:

- Where necessary that the data protection policy and privacy statement are attached to communications such as emails and letters.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

The **Data Protection Officer** 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 and anyone else covered by this policy.
- Handling Subject Access Requests.

General staff guidelines

The following are guidelines all staff should adhere to. Staff are, individually, responsible for:

- Maintaining confidential login credentials as per the company's IT Policy, which under no circumstances should be shared;

- Only accessing personal data that they need to perform their work;

- Recognising, reporting internally, and cooperating with any remedial work arising from personal data breaches;

- Not informally sharing personal data;

- Updating personal data if it is found to be out of date. If it is no longer required for the purpose it was initially used for; it should be deleted or disposed of appropriately.

- Only erasing or anonymizing personal data at the instruction of the data subject or in line with the appropriate retention period; and

- Recognising, reporting internally, and cooperating with the fulfilment of data subject access requests.

If you wish to exercise your rights, please email us at compliance@whiteandcompany.co.uk or write to us at:
FAO Data Protection Officer
White & Company
International House, Unit G
Bar End Ind. Est.
Winchester SO23 9NP

Acknowledgment

By signing below, I agree to the following terms:

I have received and read as copy of the “Data Protection Policy” and understand the same;

Employee signature: _____

Employee name: _____

Date: _____