# Data Protection Policy

# Watkin Jones & Son Ltd

# Data Protection Policy

## 1. Introduction

This Data Protection Policy (this "Policy") sets out how Watkin Jones & Son Limited ("we", "us", "our") handle the Personal Data we process in the course of our business activities.

This Policy applies to all Watkin Jones & Son Limited employees and workers ("Personnel" "You", "Your"). Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.

This Policy has been prepared with due regard to the General Data Protection Regulation (EU Regulation 2016/679) ("GDPR") and the Data Protection Act 2018.

This policy should be read together with the following related documents:

a) Data Protection by Design & DPIA Policy

b) Personal Data Retention Policy

c) Information Security Policy

d) Data Subject Rights Procedure

e) Data Breach Procedure

f) DPIA Procedure

## 2. Policy Statement

Watkin Jones & Son Limited recognises the importance of respecting and protecting the privacy of individuals with whom we work, including our employees, customers, suppliers and other third parties. We are committed to the fair, lawful and transparent processing of Personal Data and to respecting the rights of individuals whose personal information we process.

Our data protection strategy is to process personal data in a manner consistent with our strategic business objectives. We have a low appetite for risk when working with personal data.

## 3. Scope & Responsibilities

This Policy applies to all Personal Data processed by Watkin Jones & Son Limited whether held in electronic form or in physical records, and regardless of the media on which that data is stored. All Personnel are required to read, understand and adhere to this Policy.

The Directors are responsible for implementing and enforcing this Policy.

The Data Protection Management Group (DPMG) is accountable for data protection and information security governance and assurance for Watkin Jones & Sons on behalf of the Watkin Jones Group Board of Directors.

All line managers are responsible for ensuring that Personnel under their management are made aware of and adhere to this Policy.

All personnel working with personal data over which they have decision making authority are responsible for ensuring it is kept securely, is accessible only to those who need to use it and is not disclosed to any third party without appropriate authorisation.

The Data Protection Manager (DPM) is responsible for managing data protection risks, compliance obligations and for supporting Data Protection Champions (DPC).

Data Protection Champions help facilitate GDPR and data protection awareness, compliance and risk management in their specific business function.

An Outsourced Data Protection Officer ("DPO") will provide expert level advice and support to the DPM as well as meeting the statutory obligations of a DPO and is responsible for monitoring compliance with this Policy, with associated policies and procedures and with the GDPR.

If you have any questions about this Policy or about data protection at Watkin Jones & Son Limited, you should contact the Data Protection Manager who can be contacted on compliance@watkinjones.com.

Watkin Jones & Son Limited is registered as a data controller with the Information Commissioner's Office having registration number Z1850350.

## 4. Definitions

"Personal Data"means any information relating to an identified or identifiable natural person (a "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"Process" or "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Special Category Personal Data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

## 5. Data Protection Principles

Watkin Jones & Son Limited is committed to adhering to the data protection principles set out in the GDPR and shall process Personal Data strictly in accordance with this Policy.

a) Lawful, Fair & Transparent Processing

Watkin Jones & Son Limited will only process Personal Data where it is lawful for us to do so in accordance with the GDPR. We will only process special category Personal Data where is it lawful for us to do so and where permitted by the GDPR.

Data Subjects must be provided with information notifying them of the purposes for which Watkin Jones & Son Limited will process their Personal Data (a "Privacy Notice"). When Personal Data is obtained directly, the Privacy Notice shall be provided to the Data Subject at the time of collection. When Personal Data is

obtained indirectly, the Privacy Notice shall be provided to the Data Subject no later than one month after obtaining the Personal Data.

Privacy Notes must include information required by the GDPR at Articles 13 and 14 including (without limitation) the identity and contact details for the data controller and, where applicable, it's Data Protection Officer; the purpose(s) for which the Personal Data is being collected and will be processed; the legal basis justifying collection and processing and details of the length of time the personal data will be held (or, where there is no predetermined period, details of the criteria used to define that period).

b) Purpose Limitation

The processing of Personal Data must match the description given in the Privacy Notice. Where the lawful basis for processing is Watkin Jones & Son Limited's legitimate interests, we may only process the Personal Data if our legitimate interests are not outweighed by the interests, rights and freedoms of the Data Subjects in question. A legitimate interests assessment must be performed to confirm this.

c) Data Minimisation

We must collect and process no more Personal Data than is strictly necessary for the purposes of the processing ("data minimisation") as set out in the Privacy Notice provided to the Data Subject and ensure that data minimisation continues to be applied throughout the lifetime of the processing activities.

d) Accuracy

We must ensure Personal Data is kept accurate and up-to-date. The accuracy of Personal Data must be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date information is found, all reasonable steps are to be taken without delay to amend or erase that information, as appropriate.

e) Storage Limitation

Personal Data must not be kept for any longer than is necessary for the purpose for which that data was originally collected. When the data is no longer required, all reasonable steps must be taken to securely dispose of it without delay. The retention periods for different data sets are set out in the Watkin Jones Data Retention Policy.

f) Integrity & Confidentiality

Personal Data must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

## 6. Accountability

Watkin Jones & Son Limited is responsible for meeting and demonstrating compliance with its data protection obligations as set out in the GDPR.

a) Records of Processing

Where required to do so by the GDPR, we will keep written internal "Records of Processing Activities" in respect of all Personal Data collection, holding, and processing. Our Records of Processing Activities shall

incorporate the information required by the GDPR at Article 30. The RoPA will incorporate the following information:

- The name and contact details of the data controller, its Data Protection Officer and any joint controllers,
- The purposes for which we process personal data,
- Details of the categories of personal data collected, held, and processed by us; and the categories of data subject to which that personal data relates,
- Details (and categories) of any third parties that will receive personal data from us,
- Details of any transfers of personal data to countries outside the European Economic Area ("EEA") including all mechanisms and security safeguards,
- The envisaged retention periods for the different categories of personal data; and
- Descriptions of the technical and organisational measures we have implemented to ensure the security of personal data.

b) Data Protection Officer

Watkin Jones & Sons has appointed an external, independent Data Protection Officer (DPO) for monitoring implementation and compliance with GDPR. The current Data Protection Officer is Evalian Limited, telephone: 03330 500 111, email: dpo@evalian.co.uk.

c) Data Protection by Design

We will implement data protection by design and by default when processing Personal Data. This will include implementing suitable organisational and technical safeguards to reduce the risks to Data Subjects associated with our processing activities. Safeguards will be implemented during the design, implementation and lifetime of processing activities. Organisational safeguards shall include awareness training for all personnel and suitable policies and procedures relating to the processing of Personal Data. This risk led approach to data protection will be applied across all business activities to ensure data protection by design and by default, as set out in the Data Protection by Design & DPIA Policy.

d) Data Protection Impact Assessments

Where the risks to rights and freedoms of data subjects associated with any existing or planned personal data processing to be carried out are potentially high or where otherwise required by applicable law or a data protection authority in a member state in which we operate, we will carry out a Data Protection Impact Assessment ("DPIA"). All DPIAs are to be undertaken as set out in the Data Protection by Design & DPIA Policy. A record of DPIAs shall be kept, to include details of the outcome, the names of the parties signing off the DPIA recommendations and the date of next review.

e) Data Processor Contracts

Where we utilise a data processor, we will put a binding contract in place between Watkin Jones & Son Limited and the data processor to include, as a minimum, the contract terms required by the GDPR at Article 28.

f) Access to Data

Only those personnel that need access to, and use of, personal data in order to carry out their assigned duties correctly will be permitted access to personal data we hold. All personnel handling personal data on our behalf of must be:

- Made fully aware of their individual responsibilities under this policy and applicable law, and be provided with a copy of this policy,
- Appropriately trained to do so and suitably supervised, with training to be provided upon starting with and refresher training to be provided at least annually, and

All consultants, agencies and other parties working on our behalf and handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as applicable to our personnel.

## 7. Data Subject Rights

In addition to the right to be informed, which is facilitated by providing Privacy Notices as set out above, the GDPR grants specific rights to data subjects in respect of the personal data collected and processed by Watkin Jones & Son Limited as a data controller.

a) Right of Access

More commonly known as Subject Access Requests or "SARs", Data Subjects have the right to request and obtain from information relating to, and to receive a copy of, their Personal Data.

b) Right to Rectification

Data Subjects have the right to obtain the rectification or completion of inaccurate or incomplete Personal Data concerning him or her.

c) Rights to Erasure, Restriction, Data Portability and to Object

In certain circumstances and, in some cases, subject to specific exceptions, Data Subjects have the right to:

- Obtain the erasure of Personal Data concerning him or her,
- Obtain the restriction of processing of Personal Data concerning him or her,
- Obtain the Personal Data concerning him or her, which he or she has provided to us as a data controller, to transmit to another data controller without hindrance to have us transfer the personal data directly to another data controller where technically feasible,
- Object at any time to processing carried out in our legitimate interests, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or carried out for direct marketing purposes.

d) Automated Decision Making

Data Subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significantly affects concerning him or her.

e) Facilitating Data Subject Rights

Watkin Jones & Son Limited is required to provide information on the action we have taken to facilitate a request or, where applicable, the reasons for not taking action (and the data subject's right to lodge a complaint with the ICO and to seek a judicial remedy) within one month of receipt of the request. The GDPR permits us to extend this period by a further two months in certain circumstances. Requests by data subjects to exercise their rights must be facilitated as set out in the Data Subject Rights Procedure.

Because of the importance of facilitating data subject rights and to ensure we meet the deadlines for responding to requests, you must communicate receipt of a request from a data subject to exercise their rights without delay, by sending an email with details of the request to compliance@watkinjones.com.

A template for a Subject Access Request can be found in Schedule 1 of the Data Subject Rights Procedure.

## 8. Retention & Disposal

Personal Data shall not be retained for longer than is reasonably required, and in any event only for as long as set out in the Watkin Jones & Son Limited Data Retention Policy.

Once Personal Data records have reached the end of their life, they must be securely destroyed in a manner that ensures that they can no longer be used. Hard drives of redundant computers should be removed and destroyed before disposal if they have been used to hold Personal Data.

## 9. Security, Integrity & Confidentiality

Watkin Jones & Son Limited shall implement appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of Personal Data. Such measures shall be proportionate to the risks to Data Subjects associated with the processing activities in question, and shall include (without limitation):

- Encryption and pseudonymisation of Personal Data where appropriate,
- Policies relating to information security, including the secure processing of Personal Data,
- Information security awareness training, including the secure handling of Personal Data,
- Business continuity and disaster recovery capabilities to ensure the ongoing availability of and access to Personal Data, and
- Processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented to ensure the security of the processing.

## 10. Data Breach Notification

Personal Data breaches must be reported immediately to the Data Protection Manager by emailing compliance@watkinjones.com.

The Information Commissioner's Office must be notified of the breach within 72 hours after having become aware of it, if the breach is likely to result in a risk to the rights and freedoms of Data Subjects. Data Subjects must be notified of the breach without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

All data breaches, including those which do not require notification to be provided to the Information Commissioner's Office, must be handled strictly in accordance with the Data Breach Procedure and added to the Watkin Jones & Son Limited register of data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

## 11. International Transfers

Watkin Jones & Son Limited will only transfer ('transfer' includes making available remotely) Personal Data to countries outside of the EEA where:

- The transfer is to a country (or an international organisation), that the European Commission has determined ensures an adequate level of protection,
- Standard contractual clauses adopted by the European Commission have been put in place between Watkin Jones & Son Limited and the entity located outside the EEA,
- binding corporate rules have been implemented, where applicable, or
- the transfer is otherwise permitted by the GDPR.

## 12. Protection of Personal Data

All personnel must comply with the following when working with personal data:

- Personal data must be handled with care at all times and must not be shared with any colleague, who does not have access to it, or with any third party without authorisation,
- Physical records must not be left unattended or on view to unauthorised employees, agents, contractors or other parties at any time and must not be removed from the business premises without authorisation,
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it,
- All physical copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked filing cabinet, drawer, box or similar,
- All electronic copies of personal data are to be stored securely using passwords which are changed regularly, and which do not use words or phrases that can be easily guessed or otherwise compromised,
- Personal data must not be transferred to any device personally belonging to an employee or transferred or uploaded to any personal file sharing, storage, communication or equivalent service (such as a personal cloud service),
- Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this policy and the law (which may include demonstrating that all suitable technical and organisational measures have been taken and entering in to a data processor contract),
- All personal data stored electronically shall be backed-up regularly and securely, and

- Under no circumstances must any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

In addition to the obligations set out above, all personnel involved in processing personal data are required to read and adhere to the Information Security Policy.

## 13. Implementation & Policy Management

This procedure shall be deemed effective as of 22nd September 2020 and shall be reviewed annually by the Data Protection Management Group and following any significant data breach.

## 14. Document Management

| | |
|---|---|
| **Document Classification:** | Data Protection Policy |
| **Version:** | 1.1 |
| **Document Author:** | Tom Bryant |
| **Document Owner:** | Miles Littlewood |
| **Approved By:** | Oli Worrall |

## 15. Version & Revision History

| Version | Date | Author | Summary of Revisions |
|---|---|---|---|
| 1.0 | 25/05/2018 | Tom Bryant | Issue date |
| 1.0 | 25/05/2019 | Miles Littlewood | Annual review. No changes |
| 1.1 | 22/09/2020 | Miles Littlewood | Cross reference to new policies and formation of Data Governance Management Group |
| | | | |
| | | | |
| | | | |