Willmott Dixon

Data Protection Policy

Introduction

Willmott Dixon complies with all applicable laws in connection with processing data, including the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018. Data users are obliged to comply with this policy when processing Personal Data.

Definitions

- "data" is information which is held electronically or in a paper-based filing system.
- "Data Subjects" includes all living individuals about whom we hold Personal Data.
- "Personal Data" is data relating to a living individual who can be identified from that data (or in combination with other information in our possession). It can be factual (such as a name, employee number or date of birth) or it can be an opinion about that person, their actions and behaviour.
- "Data Controllers" are the decision-makers about the processing of Personal Data. They exercise control over the purposes and means of any processing.
- "Data Processors" process Personal Data on the instruction of a Data Controller.
- "Data Subject" the individual to which the Personal Data relates.
- "Data Users" are those whose work involves processing Personal Data.
- "Processing" is any activity that involves use of Personal Data. It includes collecting, recording or holding the Personal Data or organising, amending, retrieving, using, disclosing, erasing or destroying it. It also includes transferring Personal Data to other parties.
- "Special Category Personal Data" includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, genetic data or biometric data, physical or mental health or condition or sexual life or sexual orientation (and such other categories as may be added from time to time). It can only be processed under certain conditions.
- "DP Legislation" is law, regulation or directive that applies in the UK with respect to data processing. This includes the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR).

Data protection principles

Anyone processing Personal Data must comply with the seven (7) principles within DP Legislation. These provide that Personal Data must be:

Processed fairly, lawfully and transparently

Personal Data must be processed in a way that is not unduly detrimental, unexpected or misleading and may only be processed if there is a legal ground for that processing.

The processing:

i. Must be necessary for the performance of a contract or
ii. Must be necessary to comply with a legal obligation (whether under common law or a statutory obligation) or
iii. Conducted in connection with or for the purposes of protecting a legitimate interest (and balanced against the rights and freedoms of individuals) or

iv. The Data Subjects' vital interests (for example contacting a family member in the case of an emergency); or
v. Conducted following the consent or permission of the Data Subject (either by a statement or positive action to that effect) to process their Personal Data. Note that Special Category Personal Data requires the explicit consent of the Data Subject.

If the processing you are considering does not fall under one of the conditions above, please contact the Legal Department for further guidance.

Personal Data must be processed in a transparent manner and individuals must be informed or aware as to how their Personal Data is processed.

When Special Category Personal Data is required to be processed, additional conditions to those set out above must also be met. If you are intending to process Special Category Personal Data, please contact the People Team.

Processed for a specified purpose(s)

- The purpose(s) of the Processing must be clear from the start and must be recorded.

Minimised

- The Personal Data which is collected and processed must be relevant and limited to what is necessary to fulfil the stated purpose(s) of the Processing.

Accurate

- Steps must be taken to maintain the accuracy of Personal Data, including correcting information that is incorrect or misleading. Willmott Dixon employees are responsible for checking and updating their Personal Data held by Willmott Dixon and must notify the People Team immediately of any changes.

Not kept longer than necessary for the purpose

- Only keep the data for the period for which it is needed to be kept.

Data should be processed securely

- All Personal Data is classified as 'Confidential'. This means that Personal Data must be kept secure. Data Users must employ reasonable security measures including, where appropriate and/or relevant:

i. Access control (into a building and/or a floor)
ii. Physical storage locking controls
iii. Electronic folder restrictions
iv. Encryption
v. Approved file transfer methods
vi. Secure Personal Data destruction

Data Users are required to adhere to Willmott Dixon's Information Security Policy.

Accountability

- Willmott Dixon takes responsibility for complying with its obligations

Personal Data must be processed in a manner that will enable the Willmott Dixon Group to demonstrate that it meets each of the seven (7) principles.

Privacy Notices

Willmott Dixon has two Privacy Notices which apply to those who interact with it: one applies to Willmott Dixon's employees and other to third parties.

Transferring Personal Data outside the UK

Group IT must provide approval when a transfer of Personal Data outside the UK is proposed. There are certain conditions to the transfer, including ensuring that the Data Subject's rights are maintained.

Data sharing

Personal Data may be shared with any entity within the Willmott Dixon Group, or externally, only for legitimate purposes and provided that the Data Subject has been informed that it may be shared and the purposes for which it may be shared.

Personal Data may only be disclosed externally (i.e. to third parties) if there is a legal basis (for example, a legitimate interest, legal obligation or to comply with a contract) to do so.

Before sharing Personal Data, there are a likely to be a number of factors that we will consider before sharing it, including:

i. The objective – this will help to provide clarity on what data needs to be shared, if any, and to whom.
ii. What data is required – the data that is shared must be minimised to the data that is required
iii. Recipients – data should only be shared on a 'need to know' basis
iv. Frequency of data sharing – Personal Data should not be shared more frequently than necessary.
v. Mode of sharing – data should be shared in a secure manner
vi. Risk of sharing Personal Data – we will consider the risks to the Data Subjects
vii. Anonymising data – we will consider if the objective can still be achieved by anonymising data
viii. Transfer of data outside the UK – Personal Data must not be transferred outside the UK without authorisation from IT

Data transmission

Data transmission is the transfer of data (physical or electronic) from one location to another. Physical transfer of data carries with it greater risk due to the inherent lack control in the event of a potential data breach. Accordingly, physical data transfers should only be carried out where there is no electronic alternative available or if it would not be practical to transfer the data in another manner.

The duration of the transit period, when transferring from one Willmott Dixon location to another, should be kept to a minimum to lower the risk of a potential data breach. Physical data must be transferred or transmitted in a secure manner.

Where electronic transfer is appropriate, it is required to be transferred securely and through a Willmott Dixon approved means of transfer such as OneDrive.

Data Retention

We will not keep Personal Data for longer than is necessary for the purpose(s) or for which it was collected. We will take all reasonable steps to destroy or erase from our systems all Personal Data which is no longer required.

Video images – CCTV

CCTV is generally regarded as a privacy intrusive method of monitoring and should therefore be considered for use once other alternative options (that may be less intrusive) have been considered and are deemed unsuitable or not sufficiently effective or efficient.

The appropriateness of any CCTV systems should be reviewed periodically to check that their use remains appropriate and that they meet the purpose for which they were installed.

Before installing CCTV, Group IT must be contacted, and data privacy risks must be assessed. The system must be operated in a way that is consistent with the rights and freedoms of individuals (i.e. does not cause harm to individuals). CCTV must be located at strategic points and must be positioned to capture images of interest.

Static CCTV should be located on or in the immediate vicinity of or pointed towards Willmott Dixon property (or the property of the client where we are working) or, where operated on vehicles, specifically towards the area that is being monitored. Appropriate and legible signs must be placed in sufficiently prominent locations to inform those whose images may be captured that CCTV is in operation.

Drones

Drones may be operated in limited circumstances and in certain locations. The primary purpose must be in connection with enhancing commercial operations rather than a collection of Personal Data.

Users are required to comply with all applicable laws (including those from the Civil Aviation Authority) relating to the use of unmanned aircraft and any licencing requirements. Where specific permissions are required, users are required to obtain and comply with those permissions.

Before considering use of drones, please contact your Group IT. Data privacy risks must be assessed.

Data Subject's rights under DP Legislation

We will process Personal Data in accordance with Data Subjects' rights and, in particular, their right to:

i. Request to have inaccurate data amended
ii. Request access to any data held about them by a Data Controller
iii. Be informed about how their Personal Data is processed
iv. Prevent the processing of their data for direct-marketing purposes
v. Object to the processing of their Personal Data in certain instances
vi. Restrict the processing of their Personal Data in certain instances
vii. Withdraw their consent in the case where consent had previously been granted
viii. Request erasure in certain instances

With the exception of (i), please consult with Group IT to consider the request from the Data Subject(s).

Information Commissioner's Office (ICO) registration

The ICO maintains a public register of all Data Controllers registered to process Personal Data. The Legal Department manages and maintains the ICO registrations.

Data breaches and complaints

A data breach means a breach of security leading to the deliberate, accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, Personal Data. For example:

i. Unauthorised deletion of data
ii. Sending data to an unintended recipient
iii. Access to data by an unauthorised individual
iv. Sending Willmott Dixon confidential data to a personal email address for non-business use
v. Loss or theft of a laptop
vi. Alteration of data without permission
vii. Misplacing data
viii. Cyber attack
ix. Not managing Data Subjects' rights appropriately.

It is important that we deal with any data incident as soon as possible to effectively manage the incident. As such, please notify the Legal Department of which the Data Protection Officer (the DPO) is a member immediately after becoming aware of any data incident. Please do not communicate details of the incident outside of those managing the data security incident without first contacting the DPO.

The DPO, together with other relevant stakeholders, will consider the potential data breach and determine the course of action to take.

April 2026