

DATA PROTECTION POLICY

Introduction

Lee & Kan Solicitors ('the Firm') is required to comply with the law governing the management and storage of personal data, which is outlined in the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act.

For this reason, protection of personal data and respect for individual privacy is fundamental to the day-to-day operations of the Firm.

Compliance with the GDPR is overseen by the UK data protection regulator which is the Information Commissioner's Office (ICO). The Firm is accountable to the ICO for its data protection compliance.

Purpose

This policy aims to protect and promote the data protection rights of individuals and of the Firm, by informing members and everyone working for and with the Firm, of their data protection obligations and of the Firm procedures that must be followed in order to ensure compliance with the GDPR.

Scope

This policy applies to all members, staff (including managers), consultants and any third party to whom this policy has been communicated.

This policy covers all personal data and special categories of personal data, processed on computers or stored in manual (paper based) files.

Responsibility

The person responsible for monitoring the Firm's compliance with this policy is Dominic Lee ('Data Protection Officer').

GDPR

The GDPR is designed to protect individuals and personal data which is held and processed about them by the Firm or other individuals.

The GDPR uses some key terms to refer to individuals, those processing personal data about individuals and types of data covered by the Regulation. These key terms are:

Personal data

Means any information relating to an identified and identifiable natural person (**'data subject'**)

This includes for example information from which a person can be identified, directly or indirectly, by reference to an identifier i.e. name; ID number; location data; online identifiers etc.

It also includes information that identified the Clients' Organisation or business name, contact information of a client (e.g. address, email address, telephone number), case name, case details (which may include personal information relating to the Client;

special categories of data, such as medical, rehabilitation, sexual orientation, social care history and records; details of religious or other beliefs, details of any relevant criminal convictions; and details about actual and potential witnesses in the case) and fee and/or billing details.

For the Firm's purposes, clients and staff are data subjects (other individual third parties concerning whom we hold personal data about are also likely to be data subjects).

Controller

Means the natural or legal person, public authority, agency or other body who alone or jointly with others, determines the purposes and means of processing the personal data. In effect, this means the controller is the individual, organisation or other body that decides how personal data will be collected and used.

For the Firm's purposes, this Firm is a data controller for certain categories of data.

Processing

Means any operation which is performed on personal data 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.

For the Firm's purposes, everything that we do with client information (and personal information of third parties) is 'processing' as defined by the GDPR. This processing will often be in the capacity as a Data Processor on behalf of a member of staff as a Data Controller.

Special categories of personal data

Means personal data revealing:

- a) racial or ethnic origin;
- b) political opinions;
- c) religious or philosophical beliefs;
- d) trade-union membership;
- e) the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person;
- f) data concerning health or data concerning a natural person's sex life or sexual orientation

N.B. data relating to criminal convictions and offences is not included within the special categories. However, there are additional provisions for processing this type of data (see Regulation 10 of GDPR)

Data Protection Principles

The GDPR is based around 8 principles which are the starting point to ensure compliance with the Regulation. Everybody working in for and with the Firm must adhere to these principles in performing their day-to-day duties. The principles require the Firm to ensure that all personal data and sensitive personal data are:

- (a) Processed lawfully, fairly and in a transparent manner in relation to the subject (**'lawfulness, fairness and transparency'**)
- (b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**'purpose limitation'**)
- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**)
- (d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy'**)
- (e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed (**'storage limitation'**)
- (f) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures (**'integrity and confidentiality'**)

The Firm must be able to demonstrate its compliance with (a) – (f) above (**'accountability'**)

Processing personal data and sensitive personal data

You must process all personal data in a manner that is compliant with the GDPR, in short, this means you must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

You must ensure that you are aware of the difference between personal data and special categories of personal data and ensure that both types of data are processed in accordance with the GDPR.

The conditions for processing special categories of personal data that are most relevant to the Firm are:

- Explicit consent from the data subject;
- The processing is at the instruction of the Firm who is the Data Controller of that personal data;
- The processing is necessary for the purposes of carrying out the Firm's obligations in respect of employment and social security and social protection law;
- The processing is necessary to protect the vital interests of the data subject or another person;
- The processing relates to personal data that has already been made public by the data subject; or
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Rights of the data subject

The GDPR gives rights to individuals in respect of the personal data that any organisations hold about them. Everybody working for the Firm must be familiar with these rights and adhere to the firm's procedures to uphold these rights.

These rights include:

- Right of information and access to confirm details about the personal data that is being processed about them and to obtain a copy;
- Right to rectification of any inaccurate personal data;
- Right to erasure of personal data held about them (in certain circumstances);
- Right to restriction on the use of personal data held about them (in certain circumstances);
- Right to portability – right to receive data processed by automated means and have it transferred to another data controller;
- Right to object to the processing of their personal data.

If anybody receives a request from a data subject (a client or other third party concerning whom we hold personal data) to exercise any of these rights, the request must be referred to the Data Protection Manager immediately or to the Partner in his/her absence.

Note: we only have one month to respond to a request to access a copy of personal data.

Confidentiality and data sharing

The members of the Firm must ensure that they only share personal information with other individuals or organisations only where they are permitted to do so in accordance with data protection law.

Wherever, possible you should ensure that you have the client's (or other data subject's) consent before sharing their personal data, although, it is accepted that this will not be possible in all circumstances, for example if the disclosure is required by law.

Data Protection Impact Assessments (DPIAs)

DPIAs are required to identify data protection risks; assess the impact of these risks; and determine appropriate action to prevent or mitigate the impact of these risks, when introducing, or making significant changes to, systems or projects involving the processing of personal data.

In simpler terms, this means thinking about whether the Firm is likely to breach the GDPR and what the consequences might be, if the Firm uses personal data in a particular way. It is also about deciding whether there is anything that the Firm can do to stop or, at least or minimise the chances of any of the potential problems identified, from happening.

Breaches

A data protection breach is defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

Everybody working in, for and with the Firm has a duty to report any actual or suspected data protection breach without delay to their line manager and the Data Protection Manager. Full details of the Firm’s breach reporting policy can be found in the shared drive with the GDPR Policies and Forms folder.

Breaches will be reported to the Information Commissioner’s Office (ICO) by the Data Protection Manager without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, unless the Firm is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

The Data Protection Manager will maintain a central register of the details of any data protection breaches.

Complaints

Complaints relating to breaches of the GDPR and/ or complaints that an individual’s personal data is not being processed in line with the data protection principles should be referred to the Data Protection Manager without delay.

Penalties

It is important that everybody working for the Firm understands the implications for the Firm if we fail to meet our data protection obligations. Failure to comply could result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- Suspension/ withdrawal of the right to process personal data by the ICO;
- Loss of confidence in the integrity of the business’s systems and procedures;
- Irreparable damage to the business’s reputation.

Changes to our Policy

We may make changes to this Data Protection Policy at any time. The most updated version of this policy will always be posted on this webpage. We recommend that you revisit this page regularly in order to remain up to date on our policy.

