Chambers of Glen Hodgetts - Egalitylaw.co.uk

DATA PROTECTION POLICY

General Data Protection Regulation ("GDPR")

Introduction

This Practice is required to comply with the law governing the management and storage of personal data, which is set out 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 Practice.

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

Purpose

This policy aims to protect and promote the data protection rights of individuals who have instructed Glen Hodgetts to undertake legal services, and of the Practice, by informing everyone working for and with the Practice, of their data protection obligations and of the Practice procedures that must be followed in order to ensure compliance with the GDPR.

Scope

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

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

Responsibility

Glen Hodgetts also acts as his practices' Date Protection Officer and does not delegate this function. He is responsible for monitoring the Practices' compliance with this policy.

Everyone in the Practice (and any third party to whom this policy applies to) is responsible for ensuring that they comply with this policy. Failure to do so may result in disciplinary action

DATA PROTECTION MANAGER (DPM)

Glen Hodgetts, as Data Protection Manager and Officer is responsible for:-

- Developing and implementing data protection policies and procedures;
- Arranging periodic data protection training for all staff and members which is appropriate to them;
- Acting as a point of contact for all colleagues, staff and Barristers on data protection matters;
- Monitoring Chambers' compliance with its data protection policy and procedures;
- Promoting a culture of data protection awareness;
- Assisting with investigations into data protection breaches and helping Chambers to learn from them;
- Advising on Data Protection Impact Assessments; and
- Liaising with the relevant supervisory authorities as necessary (i.e. the Information Commissioner's Office in the UK).

Glen Hodgetts has adopted electronic data storage and email solutions to give maximum security to his client's data within the constraints of needing to provide effective legal services to his clients. These include the following:-

PROTECTION OF ELECTRONIC DATA

Secure Email :

Glen Hodgetts operates a secure encrypted email portal based in the EU which is 'GDPR compliant', through which all or all sensitive information can be transferred to and from Glen Hodgetts. Please email Glen Hodgetts at **glen.hodgetts@egalitylaw.co.uk** or securely at **glen.hodgetts@egalitylaw.secure-comm.com** in order to set up your secure and individual communication stream. You will be given a direct link to your personal stream and will be able to access it after creating your own confidential 4 digit pin. The portal will send you a user name and password. Once set up, secure communication can be made by clicking on the "reply securely" button in my email to you, or via my online secure portal at:-

https://egalitylaw.secure-comm.com

Please email me normally at glen.hodgetts@egalitylaw.co.uk if you have a problem setting up your secure communication individual stream via my portal.

Glen Hodgetts' secure portal operates with click-and-PIN access, TLS connections, AES-256 encryption and multi-factor authentication for your data's protection. If you do not wish to use this secure form of email then you must consent not to do so in writing; please let Glen Hodgetts know if writing that you do not wish to use his secure portal.

Cloud Storage

The Chambers of Glen Hodgetts uses an encrypted GDPR compliant data storage portal in which confidential files are stored in a Vault. This is used to communicate large data pdf files to his clients securely through individual and personally password protected data streams. This data can only be accessed by Glen Hodgetts or the client stream for which it is intended, with click-and-PIN access, TLS connections, AES-256 encryption and multi-factor authentication for your data's protection. Cloud Vault storage is based in the EU and is GDPR compliant.

The system is operated by STAY PRIVATE LTD.

https://stayprivate.com/index.html

Other data storage

Other data is stored by Glen Hodgetts on an Apple Mac computer using the latest operating system. Data is protected by

i) secure password protection to start up and enter the computer;

ii) All files are then further encrypted using FileVault which is also password protected

iii)

Cloud storage

Any data stored in the cloud is protected by click-and-PIN access, TLS connections, AES-256 encryption and multi-factor authentication; STAY PRIVATE LTD have no access to data stored on Glen Hodgetts private data portal

Mobile data

Glen Hodgetts uses a mobile phone and will occasionally have to email a client from this device and to access data on it. Emails from this device will also use his encrypted secure portal using the StayPortal App by StayPrivate Ltd. Encrypted secure email via this secure GDPR complaint email service will be used unless clients **consent** to use otherwise less secure email.

Glen Hodgetts **mobile phone** is protected by:-

i) fingerprint access of Glen Hodgetts only;

ii) additional 6 digit code to open the phone;

iii) phone locks to lock screen in 30 seconds requiring pin or fingerprint;

iv) mobile data access to the secure portal has additional 4 pin password protection after phone lock screen is open;

v) all use of mobile email/data access function is reported electronically to Glen Hodgetts desktop in case of suspected unauthorised use;

vi) in case of theft, all data can be remotely deleted;

vii) in case of theft the mobile phone can be traced via GPS

GDPR

The GDPR is designed to protect individuals and personal data which is held and processed about them by the Practice 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 physical, physiological, genetic, mental, economic, cultural or social identity of a person. For the Practice's purposes, our clients 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 Practices' purposes, this Practice is a data controller for client 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 Practices' purposes, everything that we do with client information (and personal information of third parties) is 'processing' as defined by the GDPR.

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 or for the Practice must adhere to these principles in performing their day-to-day duties. The principles require the Practice 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 Practice 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 our Practice are:

- Explicit consent from the data subject;

- The processing is necessary for the purposes of performing a legal contract with the Data Subject, most commonly provision of legal services;
- The processing is necessary for the purposes of carrying out the Practices' 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.

If you have any concerns about processing personal data, please **contact Glen Hodgetts at glen.hodgetts@egalitylaw.co.uk** who will be happy to discuss matters with you.

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 Practice must be familiar with these rights and adhere to the Practices' 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 **Glen Hodgetts** immediately on 07966 495 468 or by email at glen.hodgetts@egalitylaw.co.uk

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

Confidentiality and data sharing

The Practice must ensure that it only shares personal information with other individuals or organisations where it is 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.

Any further questions around data sharing should be directed to Glen Hodgetts on 07966 495 468 or at glen.hodgetts@egalitylaw.co.uk

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

DPIAs will be undertaken by **Glen Hodgetts.**

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 for the Practice has a duty to report any actual or suspected data protection breach without delay Glen Hodgetts in accordance with the Chambers of Glen Hodgetts Date Protection Breach Policy which can be found on his website site by clicking on the link at the bottom of this page:-

http://glenhodgetts.com/contactpoliciesgdpr/4571989542

Breaches will be reported to the Information Commissioner's Office (ICO) by Glen Hodgetts without undue delay and, where feasible, not later than **72 hours** after having become aware of the breach. Unless, the Practice is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

Glen Hodgetts 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 Glen Hodgetts on 07966 495 468 or by email to glen.hodgetts@egalitylaw.co.uk or by secure email to glen.hodgetts@egalitylaw.secure-comm.com without delay.

Penalties

It is important that everybody working for the Practice understands the implications for the Practice if the Chambers of Glen Hodgetts fails to meet its 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.

Note: The Practice could be fined up to €20,000,000, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

First Created: 24th May 2018

Updated on: 25th May 2018

Glen Hodgetts

Chambers of Glen Hodgetts

Saint Brandon's House,

27-29 Great George Street,

Bristol, BS1 5QT

07966 495 468

glen.hodgetts@egalitylaw.co.uk

glen.hodgetts@egalitylaw.secure-comm.com