SVARMSTRONG

regulatory law • health and safety • environment

DATA PROTECTION POLICY

Contents

Introduction

This Law Firm (Company) is required to comply with the law governing the management and storage of personal data, which is outlined in the General Data Protection Regulation 2018 (GDPR) and the Data Protection Act 1998.

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

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

Purpose

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

Scope

This policy applies to all members of 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

Stuart Armstrong is the Company's Data Protection and Information Security (DPIS) Manager. He is responsible for monitoring compliance with this policy.

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

Responsibilities within this role include:

- Developing, implementing and periodically reviewing data protection policies and procedures;
- Arranging appropriate data protection training for staff;
- Acting as a point of contact for all clients, colleagues, staff, consultants etc. on data protection matters;
- Monitoring the Company's compliance with its data protection policy and procedures;
- Promoting a culture of data protection awareness;
- Assisting with investigations into data protection/information security breaches and helping the Company 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).

GDPR

The GDPR is designed to protect individuals and personal data which is held and processed about them by the Company 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 include: Personal Data; Controller; Processing; and Sensitive Personal Data.

Personal data

Means any information relating to an identified and identifiable natural person (the **'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 identifies the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

For Company purposes, staff, clients and consultants are data subjects and other individual third parties 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 Company's purposes, the Company 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, aligning, combining, restricting, erasing or destroying.

For the Company's purposes, everything that we do with client information (and with the 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 solicitor as a Data Controller.

Sensitive categories of personal data

Sensitive categories of personal data include those revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- trade-union membership;
- The processing of genetic data or bio-metric data for the purpose of uniquely identifying a natural person;
- Data concerning health or data concerning a natural person's sex life or sexual orientation

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

Data Protection Principles

The GDPR is based around a number of principles which are the starting point to ensuring compliance with the Regulations. Everybody working for and with the Company must adhere to these principles in performing their day-to-day duties. These principles require the Company to ensure that all personal data and sensitive personal data are:

- Processed lawfully, fairly and in a transparent manner in relation to the subject ("**lawfulness**, **fairness** and **transparency**")
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("**purpose limitation**")
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("**data minimisation**")
- 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**")

- 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 (á**storage limitation**ñ)
- 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 (á**integrity and confidentiality**ñ)
- The Company must be able to demonstrate its compliance with the policies above (á**accountability**ñ).

Processing personal data and sensitive personal data

All our staff must process all personal data in a manner that is compliant with the GDPR. In short, this means we 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 we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- Handle peopleôs personal data only in ways they would reasonably expect; and
- Make sure we do not do anything unlawful with the data.

We ensure that our staff 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 Company are:

- Explicit consent from the data subject;
- The processing is at the instruction of a Solicitor/Fee Earner who is the Data Controller of that personal data;
- The processing is necessary for the purposes of carrying out the Companyôs 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.
- 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 ï 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.
- 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 businessôs

If you have any concerns about processing personal data, please contact Stuart Armstrong 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 Company will be familiar with these rights and adhere to this Policy in order to uphold these rights. If any employee 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 Stuart Armstrong.

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

Confidentiality and data sharing

The Company only shares personal information with other individuals or organisations where it is permitted to do so in accordance with data protection law. Wherever, possible our staff ensure that they have the clientõs (or other data subjectõs) 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 Stuart Armstrong.

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

DPIAs will be undertaken by Stuart Armstrong or other designated members of staff where required.

Breaches

A data protection breach is defined as ña breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processedò

Everybody working in, for and with the Company has a duty to report any actual or suspected data protection breach without delay to Stuart Armstrong. Breaches will be reported to the Information Commissionerõs Office (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, unless, the Company 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 Company 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 individualõs personal data is not being processed in line with the data protection principles should be referred to Stuart Armstrong without delay.

SV Armstrong Limited

May 2018.