Forbes Solicitors LLP Data Protection and Personal Information Management Policy

THE DPA AND UKGDPR: APPLICATION AND EFFECT

The Data Protection Act 2018 ("DPA") applies a version of the General Data Protection Regulation ("GDPR") in domestic law ("UKGDPR") and relates to the handling, processing and storage of all personal data. It regulates what the person or business holding information (known as the "Data Controller") can do with the information it holds and what access the person to whom the information relates (known as the "Data Subject") can do in terms of seeing the information and having it corrected or deleted.

The DPA relates to all personal data whether held by Forbes Solicitors LLP ("Forbes") electronically or in hard copy, and covers all processing of those personal data by all staff and Partners within Forbes whether in the office, working at other locations or outside of work. It also regulates the use by Forbes of third parties to handle personal data under instruction from Forbes, which may be as Data Processors or as separate or joint Data Controllers.

Personal Data and Special Category Data – Personal data includes employee information, client related data and any other information relating to any living individual who can be identified using that information either alone or with other information and to whom that information relates. It includes factual information and also statements of intention relating to a person.

There is a subset of special category personal data and these data are more heavily protected. The category of sensitive personal data is set out in Article 9 of the UKGDPR and it includes:

(a) the racial or ethnic origin of the data subject,

(b) political opinions,

(c) religious or philosophical beliefs,

(d) trade union membership,

(e) genetic and biometric data,

(f) information concerning health,

(g) sex life or sexual orientation.

Criminal Convictions and Offences

Information in this category is governed by UKGDPR Article 10 and processing should only be undertaken by official authorities or where permitted by law.

Forbes DPA Registration Number is ZB100365

The firm is registered as a fee payer with the ICO.

The data protection public register may be viewed on the ICO website Information Commissioners - Data protection public register (ico.org.uk)

COMMITMENT TO DPA

It is the intention of Forbes Solicitors to comply with the terms of the Data Protection Act 2018 and UKGDPR. All staff who process personal data, must ensure that they do so within the terms of the DPA and UKGDPR at all times and should seek guidance from Heads of Department and the firm's Data Protection Officer if in doubt.

The firm has also signed up to the ICO's Personal Information Promise which involves further commitments to deal with personal information properly.

Responsibility - The Partnership has overall responsibility for ensuring that Forbes, as the Data Controller operates within the framework of the DPA and UKGDPR. To assist the firm in ensuring compliance, the firm has identified Daniel Milnes as the firm's "Data Protection Officer". The firm has also appointed a "Deputy Data Protection Officer" Lachlan McLean, Partner, Housing and Regeneration (Litigation). All staff have a responsibility to process all personal data in line with this Policy and the DPA principles.

Employee Personal Data - The firm will ensure that the interests of its employees are safeguarded by regularly reviewing its policy and taking account of Codes of Practice and other advice issued by the Information Commissioner.

DPA AND UKGDPR: SIX CORE PRINCIPLES

Article 5 of the UKGDPR sets out six principles on how to process personal data under the DPA and UKGDPR and the Forbes Data Protection Policy is to observe all of the data protection principles in dealing with personal data. The six principles are set out below together with guidance on how to interpret them and examples of how they can apply to the firm (shown in italics).

1. Personal data shall be processed lawfully, fairly and in a transparent manner.

(a) Processing of personal data is lawful if a condition in Article 6 of the UKGDPR is met and the conditions are:

The 6 legal reasons we may use are:

- Where the personal data needs to be processed to fulfil a contract with the individual
- Where the personal data needs to be processed so we can comply with a legal obligation
- Where the personal data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's safety
- Where the personal data needs to be processed so a public authority can perform a task carried out in the public interest, and carry out their official functions
- Where the personal data needs to be processed for our legitimate interests, or the legitimate interests of another organisation (provided the rights and freedoms of individuals are not overridden)
- The individual has freely given clear consent;

(b) in the case of special category personal data, processing is unlawful unless one of the conditions in Article 9 of the UKGDPR is met. They include:

- Where we have obtained explicit consent from the individual
- Where the individual has manifestly made the information public (e.g. by social media)
- Where legal proceedings or the operation of courts are involved
- Where the personal data needs to be processed so we can comply with a legal obligation in the field of employment or social protection law
- Where the personal data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life and it is not possible to obtain consent
- Where the personal data needs to be processed for reasons of substantial public interest (which can include a number of reasons set out in the DPA and UKGDPR).

For processing to be transparent the Data Subject should be informed what information is being obtained about them and what the firm is going to use it for. We will do this in the form of a Privacy Notice in accordance with Article 13 and 14 of the UKGDPR. Transparency also requires there to be proper recognition and respect of the rights of data subjects.

We will also maintain a Record of Processing. This will clearly outline what information is collected and from whom, the safeguards in place both technical and organisational along with our retention periods.

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The purpose of processing personal data should be one as outlined in our Record of Processing and made known to the data subject through a privacy notice or otherwise clearly communicated. Staff and partners should not use personal data held by the firm for its business purposes for their own private purposes as to do so may be a criminal offence.

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

   When obtaining personal data for work purposes, staff and Partners should obtain enough information to perform the firm's obligations properly. Where the firm obtains or holds information from or about clients or third parties that is not relevant to the work the firm is undertaking that information should not be used or disclosed in the performance of the work. The firm's ISO procedures for opening files and conducting conflict checks specify what information is required for those purposes.

   Data minimisation is also an appropriate consideration to ensure that only the essential data from among those held by the firm are used to undertake a particular task.

4. Personal data processed shall be accurate and, where necessary, kept up to date.

   The firm's ISO policies require information to be updated if circumstances change.

5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

   The firm's ISO policies address retention periods for files and the period of time for which information should be retained. This is different for different types of work and in some cases external rules require information to be retained after the firm's work is complete.

   We have procedures in place to delete, erase or destroy any information in accordance with those policies.

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

   The firm has adopted policies and procedures for dealing with data and those are part of the firm's ISO and Risk Management policies. In particular, the firm has a Data and Computer Security Policy and this is relevant for preventing unauthorised processing of personal data. Access to some personal data held by the

firm is restricted to staff and Partners with a need to access it (e.g. personnel files). The firm's case management system allows for matters and entities to be locked to restrict access and this can be an appropriate measure in some cases. All staff and Partners are responsible for taking care in the way in which they deal with personal data and examples include:

(a) *Not giving out personal contact details of colleagues where a different way of dealing with a request established to be genuine is available*

(b) *Not leaving files taken out of the office in unsafe locations.*

Data minimisation is also an appropriate consideration to ensure that only the essential data from among those held by the firm are used to undertake a particular task.

If in any doubt always seek advice from a Head of Department or the firm's DPO or where applicable the firm's IT or HR Department as appropriate.

DATA SUBJECT RIGHTS

Requests for Copies of Personal Data – a Data Subject is entitled to be informed within a month of what personal data Forbes holds about them, what it is used for, third parties with which it is shared and further information as well as the personal data itself. This request is known as a "Subject Access Request". Such Requests need to be made in writing and in the majority of cases do not involve any payment to the firm.

Note – the majority of information the firm holds on its staff, can be viewed by the individual staff member by accessing "my personal record" which is password protected, via the firm's intranet system.

Note – there are some exemptions in relation to obtaining some information and the firm does not always have to provide all of the information that it holds even where the Data Subject is referred to in it. If you receive a Subject Access Request you should inform your Head of Department and the Data Protection Officer immediately and should not deal with the Subject Access Request yourself. If the firm gives out

information that it should not have done in response to a Subject Access Request that can also contravene the DPA and UKGDPR.

Compensation for Damage / Distress – an individual who suffers damage as a result of a contravention by a Data Controller of any provision of the DPA and UKGDPR may be entitled to compensation. Compensation can be for financial loss caused by the contravention or for distress or both.

Right to Erasure (Right to be Forgotten) – a Data Subject can ask a Data Controller to delete from its records personal data of that Data Subject in some circumstances. The right is not absolute and if you receive any such request you should inform your Head of Department and the Data Protection Officer immediately and should not deal with the request yourself. If the firm deletes information that it should not have done that can also contravene the DPA and UKGDPR as well as professional rules and insurance requirements.

Right to Object to Profiling – a Data Subject can object to purely automated decisions being made which take effect without involvement of a natural person to verify the outcome.

There are further Data Subject rights to object to processing of personal data and to rectification of personal data as well as restricted use of any disputed personal data and data portability. If you are aware of any Data Subject wishing to exercise any rights you should inform your Head of Department and the firm's DPO.

Data Protection by Design and Default

We are required to implement appropriate technical and organisational measures in an effective manner. We are accountable and must be able to show compliance with the data protection principles. We will put measures in place to show that we have integrated data protection into our processing activities.

This includes:

- Implementing privacy by design when processing personal data and completing privacy impact assessments where processing presents a high risk to rights and freedoms of individuals.

- Integrating data protection into internal documents including this policy, any related policies and any privacy notices.

- Regularly training staff on data protection law, this policy, any related policies and any other data protection matters. We must maintain a record of training attendance by staff.

- Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

We will also conduct a Data Protection Impact assessment when implementing new processes or systems.

Personal Data Breaches

This is defined in the UKGDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. We will take all reasonable endeavours to ensure that there are no Personal Data Breaches.

We have put in place procedures to deal with any suspected Personal Data Breach. Please see the Data Breach Procedure for further guidance. Any suspected Personal Data Breach must be reported immediately to the DPO, Daniel Milnes in addition to any other internal reporting requirements for regulatory compliance. Where possible do this using the *Report a Breach* button on the Forbes intranet.

In the unlikely event of a Personal Data Breach occurring which meets the requirements for notification to the ICO, we will report this to the ICO within 72 hours of becoming aware of it, where the individual is at risk of damage e.g. through identity theft or a breach of confidentiality. We will also communicate with affected individuals where appropriate.

IMPLEMENTATION

The Risk Management Committee has ultimate responsibility for ensuring implementation of the policy and procedures that are related to the DPA.

The Risk Management Committee will provide a more focused forum in relation to the DPA and the ongoing review and management of the DPA within the firm. The Committee will report directly to the Forbes partners.

COMMUNICATION

The DP Policy is available to all staff, clients and suppliers of Forbes, both in hardcopy and on the Intranet site. If alternative formats of the Policy are required, please contact the Data Protection Officer.

Training will provide a means by which the Policy and supporting policies i.e. Risk Management, Quality are communicated to staff and internalised in their behaviour. All staff should attend training events related to DPA that are organised by the HR & Training Department and which will help to translate the law into working practice.

The Risk Management Committee will, from time to time, supplement approved Forbes Policy with Best Practice or guidelines on behaviour and these will be disseminated to the relevant members of staff.

OTHER OBLIGATIONS, POLICIES AND QUALITY DOCUMENTS, PROTOCOLS

Many of the firm's policies (e.g. those relating to ISO Procedures and Risk Management) address issues relevant to data protection in different contexts and the same is true of other obligations on the firm relating to the handling of information. Observance of those other obligations and policies is a part of this Policy. Those policies and procedures may not refer to Personal Data or Personal Information explicitly but they are still relevant.

An example of this is the general requirement on the firm as a result of professional standards and retainer terms to respect the confidentiality of information from and about clients, whether or not that

information contains Personal Data and/or Special Category Personal Data.

All information from and about clients should be treated as highly confidential in relation to any disclosures, handling and storage of the information.

This Policy applies throughout the firm. Where specific departments or activities of the firm require more detailed instructions or statements of best practice to address data protection issues that requirement may be addressed within departmental work instructions, risk management plans and/or data protection protocols issued under this Policy and addressing either issues of application throughout the firm or for specific departments or activities. Where any such additional documents are in effect, copies should be provided to the Data Protection Officer.

This Policy and those other policies and documents in effect from time to time together constitute the firm's Personal Information Management System. An illustration of the way in which the different policies and documents overlap is attached to this Policy.

OTHER OBLIGATIONS AFFECTING DATA PROTECTION

In some limited circumstances the firm may be required to deal with personal data in a way that is not within the normal operation of this Policy. For example, the firm's Anti Money Laundering Policy may require disclosure of certain information without client consent and that can be appropriate under the DPA if handled properly. If you face a requirement to deal with personal data in a way that may be a breach of this Policy you should seek advice from a Head of Department or the Forbes DPO.

CONSEQUENCES OF BREACH

Forbes acknowledges that the firm or individual members of staff may be held liable for criminal offences under the DPA and UKGDPR. Fines for breaches may be up to £17,000,000 where the Information Commissioner takes enforcement action and Data Subjects can claim compensation from the firm in some cases (see above).

A breach of this Policy may also expose the firm to action by professional regulatory authorities such as the SRA or FSA.

Should the firm identify a member of staff in breach of the Forbes Data Protection Policy, the individual will be taken through the firm's disciplinary and grievance procedure. A serious breach of this policy may amount to gross misconduct as well as a criminal offence.

Risk Management Committee

Forbes Solicitors

March 2024

Policy Overview