JAN SOLICITORS

DATA PROTECTION POLICY

Introduction

We hold personal data about our people, clients, contacts, and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our people understand the rules governing the use of personal data to which they have access in the course of their work. In particular, this policy requires our people to ensure that the data protection officer (DPO) is consulted before any significant new data processing activity is initiated to ensure that the relevant compliance steps are addressed.

Scope of policy

This policy applies to all people. You must make yourself familiar with this policy and comply with its terms. This policy supplements our other policies relating to privacy and IT. We may supplement or amend this policy from time to time. Any new or modified policy will be communicated before being adopted.

The law

Article 5 of the EU General Data Protection Regulation (GDPR) contains data protection principles which require that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. 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.

We need a lawful basis to process all data. Lawful bases are:

1. **Consent:** The individual has given clear consent for you to process their personal data for a specific purpose.
2. **Contract:** The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. **Legal obligation:** The processing is necessary for you to comply with the law (not including contractual obligations).
4. **Vital interests:** The processing is necessary to protect someone's life.
5. **Public task:** The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. **Legitimate interests:** The processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Responsibilities

The person with overall responsibility for data is **Ms Janet Mukiibi.**

Janet has overall responsibility for the day-to-day implementation of this policy.

We must process personal data fairly and lawfully in accordance with individual rights. This generally means that we should not process personal data unless the individual whose details we are processing has given consent or we have other legitimate grounds for processing.

Janet is responsible for:

- keeping the management committee/board/CEO [*amend as appropriate*] updated about data protection responsibilities, risks and issues;
- reviewing all data protection procedures and policies on a regular basis;
- arranging data protection training and advice for all people, board members and those included in this policy;
- answering questions on data protection from our people, board members and other stakeholders;
- responding to people and clients who wish to know which data is being held on them by the firm;
- checking and approving with third parties that handle the firm's data any contracts or agreement regarding data processing.
- ensuring that all systems, services, software and equipment meet acceptable security standards;
- checking and scanning security hardware and software regularly to ensure that it is functioning properly;
- researching third-party services, such as cloud services the firm is considering using to store or process data.
- approving data protection statements attached to emails and other marketing material;

- addressing data protection queries from clients, target audiences or media outlets;
- co-ordinating with Janet to ensure all marketing initiatives adhere to data protection laws and the firm's data protection policy.

The processing of all data must be:

- necessary to deliver our services;
- in our legitimate interests and not unduly prejudice an individual's privacy.

In most cases this provision will apply to routine business data processing activities.

Our terms of business contain a privacy notice to clients on data protection. The notice:

- sets out the purposes for which we hold personal data on clients;
- highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers;
- provides that clients have a right of access to the personal data that we hold about them.

Sensitive personal data

In most cases where we process sensitive personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, relevant, and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this or we are able to rely on our legitimate interests in the use of the data.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate, you should report this to Ms Janet Mukiibi.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the HR team so that they can update your personal records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.

Printed data shall be shredded when it is no longer needed.

Data stored on a computer shall be protected by strong passwords that are changed regularly.

Data stored on CDs or memory sticks must be locked away securely when they are not being used.

The DPO must approve any cloud used to store data.

Servers containing personal data must be kept in a secure location, away from general office space.

Data should be regularly backed up in line with the firm's backup procedures.

Data must never be saved directly to non-firm owned mobile devices such as laptops, tablets or smartphones.

All servers containing sensitive data must be approved and protected by security software and a strong firewall.

Procedure for reviewing data processing operations:

Jan solicitors will constantly review its data protection processing operations, consider that privacy and data protection issues are covered at the design phase of any systems, service, product, or process by:

- putting in place appropriate technical and organisational measures and specifically our case management system and IT safeguards designed to implement the data protection principles effectively; and
- integrate safeguards into your processing so that we meet the UK GDPR's requirements and protect individual rights. Our safeguards include safe password access, firewalls and computer monitoring systems.
- developing new IT systems, services, products and processes that involve processing personal data;
- developing organisational policies, procedures, business practices and/or strategies that have privacy implications;
- physical design of our systems with data protection in mind and
- safety first when embarking on remote working and or data sharing initiatives.

By default, we ensure that we only process the data that is necessary to achieve our specific purpose of delivering legal services to clients. We will:

- specify the data required before the processing starts,
- appropriately inform individuals and

- only process the data we need for our purpose.

In doing so, we must consider:

- adopting a 'privacy-first' approach with any default settings of systems and applications;
- ensuring we do not provide an unreal choice to individuals relating to the data we will process;
- we are not processing additional data unless the individual decides you can;
- ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and
- providing individuals with sufficient controls and options to exercise their rights.
- developing a culture of 'privacy awareness' and ensuring we are following our data protection policies and procedures;
- that those who design our systems, products and services take account of data protection requirements and assist us in complying with our obligations; and
- Our daily practice, internal processes and procedures embed data protection by design.

Data Protection Impact Assessments (DPIAs):

DPIA will help us identify and minimise data protection risks in our delivery of legal services. DPIAs will be required in certain circumstances such as;

- where the processing is likely to result in a risk to rights and freedoms of a client
- Processing is likely to result in a high risk of any nature.

We will carry out our DPIA as follows:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks
- Assessing the level of risk, to consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- We will consult our data protection officer and our processors.
- If we identify a high risk that we cannot mitigate, we must consult the ICO before starting the processing.

The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the ICO may issue a formal warning not to process the data or ban the processing altogether.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. In line with our Terms of Business. Our data retention and disposal procedures are set our in our Information management policy.

Procedure for identifying and reviewing data retention time scales:

Information will be held only if is required and disposed of in accordance with our Information retention and destruction procedure below:

Retention:

- Follow the time limit for each area of practice and case type
- Check the source of information and if a minor is involved in which case the time limit starts from when they turn 18
- Assess the importance of the information as evidence of future claims
- Establish whether there are any legal or regulatory retention requirements (including: Public Records Act 1958, Data Protection Act 2018, the Freedom of Information Act 2000, the Limitation Act 1980, the General Data Protection Regulation 2018).

Retention times:

- **Wills/Codicils**: Files shall be retained for six years after the testator has died and the estate has been wound up.
- **Trusts**: Files shall be retained for at least six years after the last action in the trust has been taken. Limitation will not run against minors until they have reached the age of 18.
- **Civil Litigation**: Files shall be retained for six years but be mindful of files involving minors or persons with a disability, where the limitation period may well be extended.
- **Commercial**: Commercial property and commercial transaction files shall be retained for 15 years as there is a greater likelihood of claims outside the primary limitation period.
- **Matrimonial**: Financial and maintenance matters shall be retained for six years, however, where the matter involves a minor, consideration should be given to extending the limitation period until they have reached the age of 18.
- **AML**: Documents and information obtained to satisfy client due diligence requirements shall be kept for a period of five years, beginning on the date on which the relevant person is made aware of the retention. We are not required to keep records for more than ten years.
- **In all other cases,** documents and information shall be kept for no more than 6 years.

Disposal:

- Non-sensitive information – can be placed in a normal rubbish bin
- Confidential information – crosscut shredded and pulped or burnt
- Highly Confidential information – crosscut shredded and pulped or burnt
- Electronic equipment containing information - destroyed using kill disc and for individual folders, they will be permanently deleted from the system.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the DPO.

Data subject access requests

Individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a data subject access request (DSAR), you should refer that request immediately to the DPO. Where appropriate, we may ask you to help us comply with those requests.

Please contact the DPO if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone electronically (e.g., via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Training

Our people will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training will be provided through in-house seminars and via online learning on a regular basis.

It will cover:

- the law relating to data protection;
- our data protection and related policies and procedures.

Completion of training is compulsory.

Conditions for processing

We will ensure any use of personal data is justified in accordance with at least one of the conditions for processing and this will be specifically documented. All people who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles in the GDPR.

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect may be subject to active consent by the individual. If so, this consent can be revoked at any time.

Data portability

Upon request, an individual should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden, and it does not compromise the privacy of others. An individual may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

An individual may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting privacy impact assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the individual, privacy settings will be set to the most private by default.

Data Processing Activities

We hold a record of data processing activities. Please see the Record of Processing Data located within the Office Manual.

Data Processing Operations

A data processing impact assessment will occur before any processing which would likely result in a high risk. A DPIA would be carried out when processing data that poses a risk to our clients health or safety in a security breach.

Managing and Reporting breaches

All people have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the breach and take remedial steps if necessary;
- maintain a register of compliance breaches;

- notify the relevant regulatory authority of any compliance failures that are material either in their own right or as part of a pattern of failures.

Once any staff member at Jan solicitors is made aware of a data breach they will take the following steps:

1. Consider whether, this poses a risk to our client's rights
2. Consider if there is a possible risk to our clients,
3. Notify Janet Mukiibi our data protection officer
4. Janet will immediately contact the Information Commissioners Office (ICO) to report the breach within 72-hours.
5. Report the breach by calling the ICO helpline Monday to Friday 9am to 5pm or report online if reporting after working hours (cyber breaches are reported online).
6. Complete the Personal Data Reporting Form (copy in the office manual)
7. The ICO will record the breach and give us advice about what to do next.

Consequences of failing to comply

Failure to comply with this policy may lead to disciplinary action under our procedures which could result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact Janet Mukiibi.

Date authored: 1st July 2021

Date reviewed: 25th July 2022

Date of next review: July 2023.