KPM DATA PROTECTION POLICY

The Role of Data Protection Officers

A DPO is a person (either internal or external) who is given formal responsibility for Data Protection compliance within a business.

Article 37(1) of the GDPR states that a DPO must be appointed if:

- The relevant data processing activity is carried out by a public authority or body.
- The core activities of the relevant business involve regular and systematic monitoring of individuals, on a large scale.
- The core activities of the relevant business involve processing of **sensitive** personal data or data relating to **criminal convictions and offences**, on a large scale.

The legal transactional business of KPM does not fall into any of the three bullet point definitions above. Therefore, the appointment of a DPO is not mandatory. KPM, however, have voluntarily agreed a DPO for ease of compliance. Karen South is the DPO and she is registered as such at the Information Commissioner's Office.

Overview of Policy

KPM is required to comply in a number of ways with the Data Protection Act 1998 (DPA 1998) and the European General Data Protection Regulation (GDPR) in respect of data privacy and security. The first of these is registration under the DPA 1998.

KPM do not process data for any purpose other than compliance with Money Laundering Regulations and legal transactional purposes. KPM do not use that data as profiling for their clients.

KPM have appropriate procedures in place to protect the security of client and employee data and to ensure personal data breaches are detected, reported and investigated effectively.

KPM will hold data in accordance with our Data Retention Policy. A copy of this can be obtained at P:LEXCEL.Policies. We will only hold data for as long as necessary for the purposes for which we collected it.

KPM is a 'data controller' for the purposes of personal data – both KPM colleagues and clients. This means that we determine the purpose and means of the processing for that data.

This policy explains how KPM will hold and process the information. It explains our clients' rights as a data subject and our colleagues'. It also explains our colleagues' obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, KPM.

KPM has mechanisms in place to assess and then report relevant breaches to the ICO where we believe the client is likely to suffer some form of damage through identity theft or confidentiality breach. We also have mechanisms in place to notify our clients where the breach is likely to result in a high risk to their rights and freedoms.

As regards transfer of data, KPM does not operate in more than one EU Member State but does transfer data outside the EU to South Africa. The reason for this is that Karen South's Paralegal, Louise Axon, is based in South Africa. KPM have ensured that there is an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The data is accessed via the KPM server and transferred to an external hard drive on Louise Axon's computer. Both the computer and the external hard drive are password protected to ensure the security of that data.

We may disclose and exchange information with Louise Axon for legal transactional purposes and for Money Laundeirng Regulations as well as for reasons necessary for the full compliance with statutory, regulatory and administrative matters.

Information may be held at our offices as described above. Information may be transferred internationally to South Africa which is a country without Data Protection laws equivalent to those in the UK. This data transfer has been explained above.

We have security measures in place to seek to ensure that there is appropriate security for the information we hold.

Data Protection Principles

Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

How we define personal data

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;

- your contact details and date of birth;

- the contact details for your emergency contacts;

- your gender;

- your marital status and family details;

- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;

- your bank details and information in relation to your tax status including your national insurance number;

- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;

- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);

- information relating to your performance and behaviour at work;

- training records;

- electronic information in relation to your use of IT systems/swipe cards/telephone systems;

- your images (whether captured on CCTV, by photograph or video);

- any other category of personal data which we may notify you of from time to time.

How we define special categories of personal data

'Special categories of personal data' are types of personal data consisting of information as to:

- your racial or ethnic origin;

- your political opinions;

- your religious or philosophical beliefs;

- your trade union membership;

- your genetic or biometric data;

- your health;

- your sex life and sexual orientation; and

- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

How we define processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;

- adaption or alteration;

- retrieval, consultation or use;

- disclosure by transmission, dissemination or otherwise making available;

- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data?

KPM will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example (and see below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;

- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;

- to monitor diversity and equal opportunities*;

- to monitor and protect the security (including network security) of KPM, of you, our other staff, customers and others;

- to monitor and protect the health and safety of you, our other staff, customers and third parties*;

- to pay you and provide pension and other benefits in accordance with the contract between us*;

- paying tax and national insurance;

- to provide a reference upon request from another employer;

- to pay trade union subscriptions*;

- monitoring compliance by you, us and others with our policies and our contractual obligations*;

- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;

- to answer questions from insurers in respect of any insurance policies which relate to you*;

- running our business and planning for the future;

- the prevention and detection of fraud or other criminal offences;

- to defend KPM in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;

- for any other reason which we may notify you of from time to time.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Karen South.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;

- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;

- where you have made the data public;

- where processing is necessary for the establishment, exercise or defence of legal claims; and

- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We might process special categories of your personal data for the purposes above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;

- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and

- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

We do not take automated decisions about you using your personal data or use profiling in relation to you.

Sharing your personal data

Sometimes we might share your personal data with our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;

- your contact details and date of birth;

- the contact details for your emergency contacts;

- your gender;

- your marital status and family details;

- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;

- your bank details and information in relation to your tax status including your national insurance number;

- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;

- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);

- information relating to your performance and behaviour at work;

- training records;
- electronic information in relation to your use of IT systems/87 access fob/telephone systems;
- your images (whether captured on CCTV, by photograph or video); and
- any other category of personal data which we may notify you of from time to time.

KPM does transfer data outside the EU to South Africa and KPM have ensured that there is an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

How should you process personal data for KPM?

Everyone who works for, or on behalf of, KPM has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy KPM's Data Security and Data Retention policies.

KPM's Data Protection Officer/Data Protection Manager, Karen South, is responsible for reviewing this policy and updating members of staff on their data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of KPM and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should not share personal data informally.

You should keep personal data secure and not share it with unauthorised people.

You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

You should use strong passwords.

You should lock your computer screens when not at your desk.

Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.

Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

Do not save personal data to your own personal computers or other devices.

Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer, Karen South.

You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

You should not take personal data away from KPM's premises without authorisation from Karen South or Matthew Stubbs.

Personal data should be shredded and disposed of securely when you have finished with it.

You should ask for help from our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

Procedure for archiving data

Fee-earners are responsible for closing client files on the computer system as soon as they are able, and for archiving the file with Microeye Services Limited where the file will be transferred digitally to a disk.

KPM can only destroy the paper file if the client agrees to destruction of the paper file and must not destroy clients' original documentation.

KPM's Terms & Conditions have a clause within them stating that we intend to archive the files onto disk and then destroy the paper file.

KPM's file closing letter must be sent out to the client, which reminds the client of the process and that the file will be archived onto disk and the originals destroyed.

The client feedback questionnaire must be sent out to the client together with the file closing letter. A stamped addressed envelope must also be sent to the client for easy return of the questionnaire.

KPM's services e-card must also then be sent out to the client with the file closing letter for marketing purposes.

When a file is understood to be 'clear' in terms of office and client balances (and pending work), it should be archived in the following manner:

- Checking the case management system to ensure that there are no balances on the file.

- If the matter is closed in terms of the handling of it, but still has balances, it should be returned to the relevant member of staff with a view to the balances then being cleared, i.e. cheque sent out to client, or client being contacted for outstanding balance.

- If the case management system does confirm that there are no balances outstanding, the file should then be gathered in a box (facing same direction) pending archiving.

- This box should be filled with files of the same status: closed in terms of handling of the matter and clear of balances.

- Information about the files should be added to the archiving folder saved centrally at: P:\1 KAREN SOUTH\Archiving\Schedules. The necessary information for the files is as follows:

    - Matter Number – e.g. A0015001
    - Surname, Initial – e.g. Adams, A
    - Matter Description – e.g. Purchase of 123 KPM Road,
    - Address – e.g. 125 Solicitors Avenue,

- The file closing form must then be completed.

- This form updates our database so that we have on the case management system the correct postal address for the clients for our ongoing marketing and sending out client newsletters. It is also a checklist to make sure that the file is closed down properly and is a chance to make sure that the services e-card and client feedback questionnaire have been sent with the file closing letter.

- The Microeye archiving certificate should be completed when the file is ready to go down to Microeye Services Limited. This certificate complies with Law Society requirements and insurers' requirements for archiving. The certificate is completed by KPM only insofar as the case management number and client details are added. It is the case management number and the client details that will appear on the disk so it is essential that the correct name and unique case management reference number are added to enable easy location of disks in the future.

- The order that the files will be photocopied and archived in is so that the certificate appears first, followed by the file closing form, followed by the clear case management ledger, followed by the file itself.

Subject access requests

Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer/Data Protection Manager who will coordinate a response.

If you would like to make a SAR in relation to your own personal data you should make this in writing to Karen South. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

Your data subject rights

You have the right to information about what personal data we process, how and on what basis as set out in this policy.

You have the right to access your own personal data by way of a subject access request (see above).

You can correct any inaccuracies in your personal data. To do you should contact Karen South.

You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Karen South.

While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Karen South.

You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

You have the right to object if we process your personal data for the purposes of direct marketing.

You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

With some exceptions, you have the right not to be subjected to automated decision-making.

You have the right to be notified of a data security breach concerning your personal data.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Karen South

You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

Personal data breaches

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

A personal data breach means a breach of security leading to the accidental, unlawful or deliberate:

- Destruction;
- Loss;
- Alteration;
- Unauthorised disclosure of; or
- Access to personal data.

A breach is more than just about losing data.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"*A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.*"

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Reporting a Breach

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

The types of breaches that require reporting to the ICO are:

- Breach of the Data Protection Act (DPA);
- A privacy and electronic communications (PECR) security breach by a telecoms or Internet service provider; or
- The unlawful obtaining of personal data (known as a Section 55 DPA breach).

The ICO website at www.ico.org.uk\for-organisations\report-a-breach contains the necessary link and forms for reporting such breaches.

www.ico.org.uk\for-organisations\improveyourpractices

If there is a breach, Matthew Stubbs or Karen South should be advised. Either or both will then determine what type of breach has occurred and what requires reporting to the ICO.

Reporting the breach to the client

If there has been a breach and the threshold in Art 34.1 GDPR has been met, then Matthew Stubbs or Karen South will advise the Data Subject of that data breach as follows:

- They will explain the nature of the breach.
- They will explain how the breach occurred.
- They will explain the steps they have taken to assess the effect of that breach.
- They will assess whether or not it is a matter that requires disclosure to the ICO.
- They will advise the client as to the likelihood and severity of the breach to their rights and freedoms.

This will be documented and notification to the Data Subject will be without undue delay.

It is the responsibility of Karen South to ensure that all partners and staff are aware of their obligations under data protection law and are provided with any update as to how they are required to support the practice in ensuring compliance.

Privacy Considerations

"*Building privacy considerations at the start of projects or initiatives that involve the processing of personal data. Thinking about privacy early on will reduce risks and avoid costly changes at a later date. It is good practice to conduct privacy impact assessments during the development testing and delivery stages of any project.*"

"*The first principle of the DPA requires that you process personal data fairly and lawfully. To ensure the processing is fair, you must be transparent about how you intend to use the data. It is good practice to include privacy notices on your website and any forms that you use to collect data. These should clearly explain the reasons for using the data including any disclosures.*"

"*The second principle of the DPA requires that you do not process personal data in any manner that is incompatible with your specified purposes. If you want to use personal data for a new or different reason that was not anticipated at the time of collection, you need to consider whether this would be fair. In practice you often need to get prior consent to use or disclose personal data for a purpose that is additional to or different from the purpose you originally obtained it for.*"

"*The EU General Data Protection Regulation (GDPR) includes rules on giving privacy information to data subjects in articles 12, 13 and 14. These are more detailed and specific than in the DPA and place an emphasis on making privacy notices understandable and accessible. Data controllers are expected to take appropriate measures. The GDPR says that the information you provide to people about how you process their personal data must be:*

- *Concise, transparent, intelligible and easily accessible;*
- *Written in clear and plain language particularly if addressed to a child; and*
- *Free of charge.*"

It is the responsibility of Karen South to ensure that:

- KPM is registered with the Information Commissioner for all necessary activities under the Act.
- There is a process of continual review to determine whether any changes in KPM's registration are required as a result of changes in the nature of the business.
- The details of KPM as registered are kept up to date.

Security Breach Notification

In accordance with Article 33 we will notify personal data breaches to the Supervisory Authority without undue delay and no later than 72 hours after having become aware of such a breach.

Should there be a notification later than 72 hours, we will give reasons for the delay.

We will specify the nature of the data breach by setting out:

- The category of the breach;
- The approximate number of data subjects affected;
- The personal data records concerned;
- The likely consequences of the breach to the individual;
- The measures taken or to be taken by KPM to mitigate the possible adverse effects.

We will document and record such data breaches. If the breach is likely to result in a high risk of adversely affecting an individual's rights or freedom, then we will notify our clients directly (Article 34).

Data Protection Privacy Impact Assessments (DPIAs)

What is a DPIA?

A DPIA is a process designed to help KPM systematically analyse, identify and minimise the Data Protection risks in a project or a plan.

KPM will consider whether or not a DPIA is necessary. In considering whether or not there is likely to be a project or plan that will involve our clients or our colleagues' data, KPM will complete the DPIA template which is found at: P:\LEXCEL\Data Protection\GDPR\Data Protection Privacy Impact Assessments.

KPM will conduct a DPIA when there is any processing that is likely to result in a high risk to the rights and freedoms of individuals.

When KPM consider the risks related to our intended processing – we will also consider our general obligation under GDPR of Data Protection by Design and Default.

At the time of determination of the means for processing and at the time of processing itself, KPM will:

- Implement appropriate, technical and organisational measures.
- Integrate the necessary safeguarding to the processing in order to meet the requirements of the Regulations and to protect the rights of Data Subjects.

The benefits of completing a DPIA for KPM:

- We will be able to identify and fix problems at an early stage.
- It can reassure our clients and our colleagues that we are protecting their interests and have reduced any negative impact on them as much as we can.
- If thought helpful, KPM will consult colleagues and clients on the process for the DPIA.
- KPM will consider whether or not to publish the DPIA to improve transparency and for our clients to understand how and why we are using their information.

A DPIA will be considered for any new project that will involve processing of data such as transfer of our archiving function or transfer of our case management system.

The DPIA will include consideration of the following risks:

- Physical, material or non-material damage resulting from the data processing.
- Whether or not the processing may give rise to:
    - Discrimination;
    - Identity theft;
    - Fraud;
    - Financial loss;
    - Damage to the reputation;
    - Loss of confidentiality of personal data protected by professional secrecy;
    - Unauthorised reversal of pseudonymisation;
    - Or any other significant, economic or social disadvantage.

Any of which may result in Data Subjects being deprived of their rights and freedoms or prevented from exercising control over their personal data.