Lux Mediation

Data Protection Policy

Introduction

This policy serves the dual purpose of being a guide to those involved in processing personal data on behalf of Jonathan Lux and also to act as the policy documenting how the Data Protection Act 2018 ("DPA") is complied with on a practical basis as a data controller.

In order to draft this policy, an information audit was carried out and this process will be repeated whenever this policy is reviewed. This process also included assessing the information required for the Data Protection Privacy Notice and it was deemed that only one notice for all categories was required; this was drafted and is version controlled at February 2021.

Status

Mr Jonathan Lux is registered as a Data Controller with the Information Commissioner's Office ('ICO') and his registration number is: ZA084920.

The legislation

On 31 January 2020 the UK ceased to be an EU Member state and was in the 'implementation period' until 31 December 2020, during which time the UK was subject to EU data protection legislation pursuant to the EU-UK Withdrawal Agreement. This included the GDPR.

When the implementation period concluded the GDPR was incorporated into the UK's domestic law as the 'UK GDPR' under the European Union (Withdrawal) Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (the DPPEC Regulations), SI 2019/419. Some related changes were made to the Data Protection Act 2018. Ultimately, this resulted in the preservation of the EU GDPR standards within UK domestic law.

Under GDPR and the Data Protection Act 2018, there are essentially 6 overriding principles:

- Lawfulness, fairness, and transparency.

- Purpose limitation, which means that:
  - An organisation should only collect personal data for specified, explicit, and legitimate purposes; and
  - Should not process the personal data in a manner that is incompatible with those purposes, except under limited circumstances.

- Data minimisation, which means that personal data should be:
  - Adequate;
  - Relevant; and
  - Limited to what is necessary for the purpose of processing.

- Accuracy, which means that personal data must be:
  - Accurate and kept up-to-date; and
  - Corrected or deleted without delay when inaccurate.

- Storage limitation, which requires that the organisation keep personal data in identifiable form only for as long as necessary to fulfil the purposes the organisation collected it for, subject to limited exceptions.

- Integrity and confidentiality, which requires that the organisation secure personal data by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

The purpose of our processing

After an internal assessment, giving consideration to all 6 lawful grounds for processing data, it is considered that there are 3 grounds which apply to the data collected and processed, they are as follows:

1. Processing is necessary for the performance of a contract, or to take steps prior to entering into a contract. The client contract is comprised of a Client Engagement Letter, Terms and Conditions - and possibly a Conditional Fee Agreement depending on the funding arrangement - which sets out the terms of the contract and the services to be provided to clients.

2. Processing is necessary for the purposes of our legitimate interests or those of clients in the provision of legal services and use in legal proceedings, except where those interests are overridden by the interests, rights or freedoms of affected individuals. In order to determine this, a number of factors will be weighed up, including what the data owner was told at the time they provided the data, what their reasonable expectations are, and the nature of the data as well as what impact it's use will have.

3. Processing is necessary for compliance with mandatory legal obligations.

Secondary processing

The DPA requires that data is only used in accordance with the lawful ground which the personal data was initially collected for. If there is an intended secondary use, then there is an obligation to assess whether the secondary use is compatible with the original purpose for which it was collected. If after such assessment, the secondary use it is not compatible, then the data subjects' specific consent must be sought to the use the data for that lawful purpose.

Assessments of this nature should be recorded clearly in a file note showing how the consideration was made and put into the assessment.

In the event of any uncertainty, Mr Lux should be consulted before the data is used for the secondary purpose.

Processing activities

The following are activities (although not an exhaustive list) which are carried out that involve processing personal data:

- Undertaking obligations arising from any contracts entered into;
- Making contact by email, fax, post or phone where contact details have been provided;
- Records of correspondence;
- Conducting checks to identify clients, verify their identity and screen for financial or other sanctions;
- Gathering and providing information required by or relating to audits, enquiries and investigations by regulatory bodies;
- Complying with professional, legal and regulatory obligations to ensure policies are adhered to;
- Operational reasons, such as improving efficiency, training and quality control;
- Ensuring the safety and confidentiality of commercially sensitive information;
- Updating and enhancing client records;
- Preventing un-authorised access and modifications to systems;
- Preparing and filing statutory returns;
- Ensuring good governance, accounting, management and auditing;
- Passing client and other relevant parties' details to experts, including medical experts and other professionals for the purposes of obtaining professional advice and complying with contractual obligations;
- Other contact in the course of providing services to clients;
- To respond to complaints;
- Credit reference checks via external credit reference agencies;
- External audits and quality checks;
- Statistical analysis to help manage processes, e.g. in relation to financial performance, client base, work type or other efficiency measures;
- Making notifications about changes to services;
- Improving products and services;
- Maintaining internal records, including about terminated contracts;
- Making internal referrals for other legal services which may be of benefit to clients;
- Marketing services;
- Providing information, products or services which are requested;
- Sending information, or newsletters and legal updates which parties may find of interest where those parties have indicated they wish to be contacted for such purposes;

- Contact during any recruitment and selection processes;
- Converting into anonymised, statistical or aggregated data which can't be used to identify parties but may be used for the purposes of statistics, research reporting and future planning for business;
- To ensure content from the website is presented in the most effective manner; and
- Other legitimate reasons, such as to enforce terms of use, or take other action required or permitted by law or for other safety and security reasons.

Location of personal data

All client files will be stored securely either electronically or in a secure office. All electronic files will be backed up on-site and off-site, using an approved supplier, with appropriate data encryption and secure storage.

Access to any network and any case management system will be secured by user-name and passwords. Any current and future employees or agents will be required to sign a confidentiality agreement.

On the occasions where client documents will need to be kept, these will be kept only for as long as necessary and then they will be returned to the client. Such documents will be retained in a secure office.

Computer equipment and data are securely stored on the premises with physical key access that can only be accessed by the owner/managers and any authorised employee. No unauthorised access is permitted.

All client confidential waste will be removed securely in accordance with the requirements of the DPA.

Categories of individuals

Personal data may be held on the following categories of individuals:

- Clients;
- Prospective clients;
- Directors, employees and consultants;
- Prospective employees and consultants;
- Members of client's families/friends;
- Witnesses;
- Other parties involved in accidents or incidents;
- Medical practitioners;
- Employees of client's employers;
- Employees of parties' insurance companies;
- Landlords and employees of landlords;
- Suppliers and employees of suppliers;

Categories of personal data

Information collected and processed may include details of the following types of information:

- Contact information (names, postal address, email address, telephone and fax numbers and preferred gender identity);
- Other personal information required in order to fulfil contractual obligations, such as: date of birth, property ownership details, bank details and other financial information and records, credit history, family relationships, national insurance number;
- Occupational information, (job status, job title, former job titles, salary, organisational associations, professional experience and qualifications, interests and preferences where these details have been provided in order to tailor information about services);
- Identification documents, including date of birth and photographic identification;
- Services in respect of which an interest has been expressed;
- Up to date record of claims to include letters and other communications (e.g. emails) with the client and other parties and dairy entries regarding the claim;
- Other information collected and used in the course of business, including information provided by clients concerning employees or those providing services to clients; or
- Where necessary and legally permitted, sensitive data, such as diversity and health data and/or details of offences and related proceedings. It is permissible to process data for establishing, exercising or defending legal rights in accordance with Schedule 1, Part 3, paragraph 33 of the DPA 2018 and this is the most likely reason why such data would be processed or to comply with professional obligations.

Categories of recipients

There are occasions where data may be shared with third party recipients in order to fulfil contractual obligations. Authority will always be sought from the client before this data is shared and this is detailed in the terms and conditions provided to the client with the Letter of Engagement.

Some of the types of third parties data may be sharedwith are:

- To other suppliers, such as expert witnesses, barristers, or other external agencies are engaged on the client's behalf. When data is provided, they are required to act in accordance with instructions and keep personal information secure with an adequate level of protection;
- To courts, tribunals and other government bodies and relevant regulators (BSB and the ICO) in connection with matters relating to provision of services;
- To professional indemnity insurers, brokers, auditors and other professional advisers;
- To clients in connection with the provision of services;
- To auditors in connection with maintenance of any quality certifications;

- To other third parties when required by law or other regulatory authority, when there is a duty to comply with legal or professional obligations (for example to comply with anti-money laundering obligations and counter terrorism measures);
- To enforce or protect rights, property or the safety of directors, staff and clients. (This includes exchanging information with other companies and organisations for the purposes of fraud prevention and detection and credit risk reduction);
- To other parties in legal proceedings, including solicitors and barristers acting on the other side of a case or transaction;
- To financial institutions providing finance for transactions.

Where data is shared under contractual agreements with third parties, a due diligence check will always be carried out and confidentiality agreement will be sought with such parties if they are not already obliged to provide this by law. Our regulations offer clients several layers of protections, including protection from third parties completing work.

Transfer to third countries

As stated above most of the time data processed is encrypted and stored on UK secure servers.

There may be rare occasions personal information may need to be transferred to countries outside of the UK which do not provide the same level of data protections. This would only ever take place to allow contractual or professional obligations to be met; wherever possible this will be done with permission. For example, in relation to legal claims with an international element, or where overseas agents need to be instructed to assist in performing legal services. In these circumstances, steps will be taken to ensure that personal information is adequately protected.

Retention schedules

Your information is only retained for as long as is necessary for the purpose for which it was obtained. This could include compliance with legal obligations (by way of example, in relation to anti money laundering regulations and the mandatory required time to keep information for). It could also include conducting legal work as instructed or establishing or defending claims which could be made against us, for example for negligence in the performance of our obligations.

In most circumstances, data will not be retained for longer than seven years which is the time required under the BSB regulations.

Security measures

As already established the majority of the data processed will be stored electronically or in a secure office. All electronic files will be backed up on-site and off-site, using an approved supplier, with appropriate data encryption and secure storage.

All employees and agents will be required to sign a confidentiality agreement.

Off-site working

When working off-site and transporting data, all barristers, employees and contractors will be aware of the security risks to personal data and confidentiality.

IT equipment

The following standards will be met in relation to IT:

- Ensure computer hardware is effective enough to give optimum protection;
- Make sure that software, including but not limited to operating systems and internet browsers are up to date and that disks are cleaned up regularly;
- Only install trusted software on to systems;
- Antivirus systems will be used and kept it up to date;
- Where possible, encryption will be used on mobile devices;
- Documents will be encrypted wherever possible;
- Software will only be installed which has been checked (and where possible, checked and approved by an IT adviser);
- Distributing files by unencrypted email attachments or flash drives/memory sticks will be avoided where possible; and
- Carrying files and ensuring information is transported on encrypted mobile devices will be done where possible, if working in transit or transporting information.

Review and monitoring

Data held and the processing of it is monitored on an ongoing basis and a formal review is carried out annually.

If necessary, after the review, this policy and our Data Protection Privacy Notice will be updated and send this out to all individuals whose data is processed.

Record of personal breaches

Any breaches during the processing of personal data are serious matters. If it is considered that the break poses a risk of harm to the data subject(s) then within 72 hours, a report must be made to a supervisory authority, namely the ICO and usually the BSB. The data subject must also be notified without undue delay.

Therefore, time is of the essence and the sooner enquiries can be carried out the better protection that can be afforded to both the data subject(s) and data controller.

Any personal breaches will be recorded within a report and maintained with this policy and will contain:

- The date of the breach;
- The name of the individual(s) whose data has been processed inappropriately;
- The impact the breach has had or may have;

- A full description of the breach including any individuals or organisations involved;
- An analysis of whether a report should be made to a supervisory authority – namely the ICO or BSB;
- Details of whom the breach was reported to and their response;
- A summary of steps taken to rectify the breach and the steps taken to ensure it does not occur again;
- Details of any compensation given as a result of thebreach; and
- Details of any fine or regulatory action taken as a result of the breach.

Ensuring individual rights are protected

General principles

Any requests by individuals in relation to their data, known as a Subject Access Request ('SAR'), will be recorded in detail whether the request is verbal or in writing or by email or letter. A decision and action notice will be prepared setting out the request (and will attach a copy of the request, if in writing). This initial record of the SAR will be dealt with and a response will be provided within one month. If a number of requests have been made or the request is complex, meaning more time is needed to properly respond, then a response will be provided within three months; however, within the initial one-month period you will be informed of the need for more time and the reasoning.

When an SAR is received, if there are any doubts about the identity of the person making the request then the identity will be verified using "reasonable means". This may involve asking the individual to confirm their identity by providing two forms of acceptable ID e.g. photographic identification such as a passport or driving licence and one form of identification with an address on from a reliable source such as a bank, utility company etc.

1. **Right to be informed**

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the DPA. Individuals will be provided with information including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. This is called 'privacy information'.

All of the details required are set out in the Data Protection Privacy Notice. The information provided to people is concise, transparent, intelligible, easily accessible, and uses clear and plain language.

Privacy information is actively provided to individuals. The link to the Data Protection Privacy Notice can be found on the website which is sent to all new clients as and when it is updated. For others whom data is held on, the Data Protection Privacy Notice is on the website in a clearly marked and accessible way.

Privacy information must be provided to individuals at the time their personal data is collected from them. Therefore, if data is received from anyone who has not previously provided their

data, they will be provided with a link to or a copy of the current Data Protection Privacy Notice; this may be handed to the person or delivered by email or post.

Personal data from other sources is not currently obtained or held, should it be in the future, the individuals that the data concerns must be provided with privacy information within a reasonable period of obtaining the data and no later than one month.

If the way data is processed changes in the future, the new use must be brought to the attention of the individual whose personal data it is, before it is processed. An impact assessment will also be conducted.

2. Right of access

Under the DPA, individuals have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information – essentially this will be the information that is contained within our Data Protection Privacy Notice.

A copy of the information will be provided free of charge. However, a 'reasonable fee' will be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive or if further copies of the same information is requested. This does not mean that there will be a charge for all subsequent SARs. Decisions will be made on fee charging on a case-by-case basis. Any fee must be based on the administrative cost of providing the information.

If the request is made electronically, the information will be provided in a commonly used electronic format.

As a provider of legal services, it is common for a lien to be exercised over client files and papers until such time as a client has settled any outstanding fees. However, a data subjects rights under the DPA overrides any right to a lien.

3. Right to rectification

The DPA includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request for rectification verbally or in writing.

If the request is made verbally, this will be recorded in a full and detailed attendance note which will be retained within records alongside this policy.

In certain circumstances a request for rectification can be refused. This right is set out in the Data Protection Act 2018 (Part 3, Chapter 2, paragraph 46) which states:

> 1. *The controller must, if so, requested by a data subject, rectify without undue delay inaccurate personal data relating to the data subject.*
> 2. *Where personal data is inaccurate because it is incomplete, the controller must, if so requested by a data subject, complete it.*
> 3. *The duty under subsection (2) may, in appropriate cases, be fulfilled by the provision of a supplementary statement.*

4. *Where the controller would be required to rectify personal data under this section but the personal data must be maintained for the purposes of evidence, the controller must (instead of rectifying the personal data) restrict its processing.*

If a request for rectification is received, reasonable steps will be taken to ensure that the data is accurate and to rectify the data if necessary. The arguments and/or evidence provided by the data subject will be considered in this regard.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort that will be put into checking its accuracy and, if necessary, taking steps to rectify it. For example, a greater effort will be made to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

4. **Right to erasure**

The DPA introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing.

Individuals have the right to have their personal data erased if:

- The personal data is no longer necessary for the purpose which it was originally collected or processed for;
- If there is no overriding contractual obligation to continue this processing;
- The personal data has been processed unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- It is necessary to comply with a legal obligation;
- The personal data was processed to offer information society services to a child.

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the DPA. Therefore, if the data collected from a child is processed, particular weight will be given to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent; or

- Whilst unlikely, in circumstances where:
  - The personal data has been disclosed to others; or
  - The personal data has been made public in an online environment (for example on social networks, forums or websites).

If the personal data is disclosed to others, each recipient will be contacted and informed of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, the individuals will be informed about the recipients.

Also, unlikely, but if personal data has been made public in an online environment reasonable steps should be taken to inform other controllers who are processing the personal data to erase

links to, copies or replication of that data. When deciding what steps are reasonable, available technology and the cost of implementation will be taken into account.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation;
- For the performance of a task carried out in the public interest or in the exercise of official authority;
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- **For the establishment, exercise, or defence of legal claims.**

As set out above, it is possible to extend the time limits by two months, however, it is the ICO's view that it is unlikely to be reasonable to extend the time limit unless:

- It is manifestly unfounded or excessive;
- An exemption applies; or
- Proof of identity has been requested before considering the request.

5. **Right to restrict processing**

Individuals have the right to request the restriction or suppression of their personal data.
This is not an absolute right and only applies in certain circumstances. When processing is restricted, it is permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing.

Individuals have the right to request the processing of their personal data is restricted in the following circumstances:

- The individual contests the accuracy of their personal data and the process of verifying the accuracy of the data is in underway;
- The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the DPA) and the individual opposes erasure and requests restriction instead;
- **The personal data is no longer needed but the individual needs it to be kept it in order to establish, exercise or defend a legal claim;** or
- The individual has objected to the processing of their data and it is being considering whether there are legitimate grounds to override those objections of the individual.

Although this is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:

- If an individual has challenged the accuracy of their data and asked for us to rectify it, they also have a right to request processing of the data is restricted while their rectification request is considered; or
- If an individual exercises their right to object, they also have a right to request the processing of the data is restricted while the objection request is considered.

Therefore, as a matter of good practice the processing of data will automatically be restricted whilst a request for rectification is being considered based on accuracy or the legitimate grounds for processing the personal data in question.

In practical terms, given that sophisticated methods for storing or processing data are not used, the decision on how to restrict processing will be made within the decision and action notice which is prepared following receipt of the request.

Following a request, no restricted data will be processed in any way except to store it unless:

- The individual consents;
- **It is for the establishment, exercise or defence of legal claims;**
- It is for the protection of the rights of anotherperson (natural or legal); or
- It is for reasons of important public interest.

If the personal data has been disclosed to others, each recipient will be contacted and informed of the restriction on processing, unless this proves impossible or involves disproportionate effort. If asked to, individuals will be informed about these recipients.

Once a decision has been made on the accuracy of the data, or whether legitimate grounds override those of the individual, the restriction may be lifted. If this is done, the individual will be informed before the restriction is lifted.

6. **Right to data portability**

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

In view of the services provided and the fact that the system in place is not operated in an overly sophisticated technological way, if a client seeks to excise this right, we will consider whether data portability is possible and how best to assist the individual. Should this request not be possible, it will be possible to treat the request as a SAR.

7. **Right to object**

The DPA gives individuals the right to object to the processing of their personal data in certain circumstances.

However, this right does not apply to the data processed here given that individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes and no direct marketing is carried out.

None of the following ways in which individuals can also object if the processing is carried out:

- A task carried out in the public interest;
- The exercise of official authority vested in you; or
- Legitimate interests (or those of a third party).

8. **Rights related to automated decision-making including profiling**

The rights contained under these provisions of the DPA do not apply as no data is processed in the following ways:

- Automated individual decision-making (making a decision solely by automated means without any human involvement); and
- Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.