MONTAGUE LEDGISTERS

Solicitors on the Green

General Data Protection Regulations

meeting the requirements

16.05.2018

41/41a Haven Green,
Ealing,
W5 2NX

Contents

Purpose of this document

The purpose is to document compliance, provide the reasoning behind the 'lawful basis' of the categories of data that are collected. Information considered and document the data audit. This document has been written in line with current guidance. As the implementation of GDPR unfolds it is envisaged that more guidance and clarification will be forthcoming both from the Law Society and from the ICO. Guidance specific to the legal industry is sparse and where guidance has been issued by the Law Society, full clarification has not really been provided for the average high street firm but advise given to refer to the ICO website which does not contain legal industry specific information. As such this document will be subject to ongoing review but will be reviewed at least annually by the Directors.

What is clear however, is the statement within the GDPR guidance issued by the ICO in relation to the Lawful Basis of Legal obligation which states *" The lawful basis for processing necessary for compliance with a legal obligation is almost identical to the old condition for processing in paragraph 3 of Schedule 2 of the 1998 Act.*

You need to review your existing processing so that you can document where you rely on this basis and inform individuals. But in practice, if you are confident that your existing approach complied with the 1998 Act, you are unlikely to need to change your existing basis for processing."

As an organisation authorised and regulated by the Solicitors Regulation Authority, we have been and are continually required to maintain compliance with numerous rules, regulations and legislation including SRA Regulations, Code of Conduct, Strict Rules of Confidentiality, the Data Protection Act 1998 (which has been replaced by GDPR) and regulatory requirements applicable to a business within the legal industry. The majority of data that we collect is in relation to providing legal services to our clients and for the most part, the lawful basis is legal obligation. We have carried out a data audit – see below which contains a description of the categories of individuals and categories of personal data and retention schedule. The organisation does not transfer data to countries outside of the UK and EU (third countries). Our technical and security measures are contained within our office manual. In terms of training and specific provisions of Data Protection & Client Confidentiality not covered in this document, reference is to be made to the relevant sections in our Office Manual.

Any request by the data subject for access to their data will be in accordance with the GDPR and will be provided within one month.

Key Information

Montague Ledgisters Solicitors are Data Controllers and Data Processors under GDPR. The general purpose of the collection and processing of data is to enable the organisation to carry out the provision of legal services. We do not carry out direct marketing digitally or otherwise. The organisation has appointed the COLP. as the person responsible for Data Protection who will carry out the DPO's task's the minimum of which is defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

Key Provisions

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) 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; personal data may be stored for longer periods insofar 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
f) 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."

Article 5(2) requires that: *"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."*

The first principle requires that you process all personal data lawfully, fairly and in a transparent manner. Processing is only lawful if you have a lawful basis under Article 6. And to comply with the accountability principle in Article 5(2), you must be able to demonstrate that a lawful basis applies.
If no lawful basis applies to the processing it will be unlawful and in breach of the first principle. Individuals also have the right to erase personal data which has been processed unlawfully.
The individual's right to be informed under Article 13 and 14 requires you to provide people with information about your lawful basis for processing. This will be included in all client care letters from 25/05/2018 and a privacy notice will be included on our website, even though we do not offer online services or collect data online. We will also notify individual of non- client related categories of the lawful basis for processing- see appendix 1 for details/time targets.

The lawful basis for your processing can also affect which rights are available to individuals. Key examples:

	Right to erasure	**Right to portability**	**Right to object**
Consent	✓	✓	**X** but right to withdraw consent
Contract	✓	✓	**X**
Legal obligation	**X**	**X**	**X**
Vital interests	✓	**X**	**X**
Public Task	**X**	**X**	✓
Legitimate Interest	✓	**X**	✓

What is personal data?

Personal data is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of the law. Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

The law protects personal data **regardless of the technology used for processing that data** – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

Examples of personal data

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Examples of data not considered personal data

- a company registration number;

- an email address such as info@company.com;
- anonymised data.

What is processing?

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the **collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination** or otherwise making available, **alignment or combination, restriction, erasure or destruction** of personal data.

The General Data Protection Regulation (GDPR) applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system.

Examples of processing

- collecting client information
- staff management and payroll administration;
- access to/consultation of a contacts database containing personal data;
- sending promotional emails*;
- shredding documents containing personal data;
- posting/putting a photo of a person on a website;
- storing IP addresses or MAC addresses;
- video recording (CCTV).

**Please remember that to send direct marketing emails, you also have to comply with the marketing rules set out in the ePrivacy Directive.*

Relevant Lawful Basis

Legal obligation

Article 6(1)(c) provides a lawful basis for processing where:
"processing is necessary for compliance with a legal obligation to which the controller is subject."

When is the lawful basis for legal obligations likely to apply?

In short, when you are obliged to process the personal data to comply with the law. Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So it includes clear common law obligations. This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute. You should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable legal obligations. The lawful basis for processing necessary for compliance with a legal obligation is almost identical to the old condition for processing in paragraph 3 of Schedule 2 of the 1998 Act. We have reviewed our existing processing to document reliance on this basis. Regulatory requirements also qualify as a legal obligation for these purposes where there is a statutory basis underpinning the regulatory regime and which requires regulated organisations to comply. We are confident that our existing approach to client and client related data complied with the 1998 Act and we will continue to be compliant under GDPR.

Where processing is on the basis of legal obligation, the individual has no right to erasure, no right to data portability, or no right to object.

Legitimate interest

Article 6(1)(f) gives you a lawful basis for processing where:

“processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

When is it likely to be used?

Legitimate interests is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

Action Plan

Action	Person responsible	Target Date
Client care letters to be updated to ensure individual’s right to be informed under Article 13 and 14 is complied with – ie: providing people with information about lawful basis for processing their data. This will be included in all client care letters from 25/05/2018 and a privacy notice will be included on our website	The COLP.	25/05/2018
All staff members to be informed of the lawful basis for processing their data	The COLP.	Asap
Non client related categories to be informed of the lawful basis for processing their data	The COLP.	As instructions issued/appointed
All staff to be reminded of the Data Protection Provisions and importance of informing the COLP. if any breach suspected.	The COLP.	Asap

Data Audit

To understand the data we collect and what our lawful basis is and in turn our responsibilities, we have carried out an audit of our data. Data that is collected from the client or as a 'by product' of the clients instructions is treated in the same way as the data is processed to comply with a common law or statutory obligation which includes the legal process and the processing is necessary and falls within the lawful basis of 'Legal Obligation'.

Data collected from or through clients

Source of Data	What Data Collected?	Why is it collected?	How is it used?	Where/How is it stored?	How long do we keep it?	How is it protected	Can we remove it?	Procedure?	Lawful Basis?
Clients	Clients Personal Data – Name Address DOB e-mail tel number ID numbers	Compliance with the Solicitors Regulation Authority Code of Conduct and Handbook, Legal Services Act, Money Laundering Regulations, Criminal Finance Act	Identification Carrying out clients instructions Progressing clients case	LEAP case management system And/or Individual Paper files	6 years after conclusion	Password protected access to database Access to paper files by staff only and kept secured in locked and secured Office. Archived files kept secured in locked and secured storage.	Client details need to be kept for mandatory conflict checks. Matter files can be deleted.	Simple deletion process Paper files re securely destroyed	Legal obligation
Clients papers/prosecution evidence/information provided by client/information provided by other side	Other side Name Address DOB e-mail tel number ID numbers								
Clients papers/information provided by client	Witnesses Name Address DOB e-mail tel number								

	ID numbers								
Clients papers/information provided by client	Partners, Next of kin, Name Address DOB e-mail tel number ID numbers	Compliance with the Solicitors Regulation Authority Code of Conduct and Handbook, Legal Services Act, Money Laundering Regulations, Criminal Finance Act	Identification Carrying out clients instructions Progressing clients case	LEAP case management system And/or Individual Paper files	6 years after conclusion	Password protected access to database Access to paper files by staff only and kept secured in locked and secured Office. Archived files kept secured in locked and secured storage.	Client details need to be kept for mandatory conflict checks. Matter files can be deleted.	Simple deletion process Paper files re securely destroyed	Legal obligaion Legal obligation
Clients papers/information provided by client	Beneficiaries or other 3rd parties Name Address DOB e-mail tel number ID numbers								
Potential Clients	Name Address e-mail tel number	To be able to respond to initial queries	Info needed to deal with initial queries	LEAP case management system/excel spreadsheet for new queries	If no progression 6 years after initial collection (to enable conflict checks)	Password protected access	Name and address to enable conflict checks	Simple deletion process	Legitimate Interest

Data Collected - other sources (not from client as source)

Source of Data	What Data Collected?	Why is it collected?	How is it used?	Where/How is it stored?	How long do we keep it?	How is it protected	Can we remove it?	Procedure?	Lawful Basis?
Directors/Partners/Staff members	Name DOB Address NI number Diversity Data Tel no Nationality/right to work	Compliance with Employment Law Regulations Recruitment procedures SRA Code of Conduct	For employment purposes Payroll PAYE/NI HMRC SRA Diversity Data Collection	HR Files – Locked cabinet Digital folder	6 years after employment ceases	Password protected access by directors only	Yes	Deletion	Legal Obligation
Directors/Partners/Staff members	Emergency Contact/Next of kin Name & Contact details	Compliance with Health & Safety Regulations	Only when necessary – in case of emergency	HR Files – locked cabinet Digital folder	When employment ceases	Password protected access by directors only	Yes	Deletion	Legal obligation
Experts/Interpreters/Barristers/Medical Experts, Consultants and other third party suppliers (Individuals)	Name Address E-mail address Tel no	Compliance with SRA guidelines Identification to ensure relevant expertise, experience and relevant qualifications	To progress clients matter/act on instructions	Stored digitally – Central Register	6 years after end of contract	Password protected access by staff only	Yes	Deletion from system	Legitimate Interest
Applicants for job vacancies	Name DOB Address NI number Diversity Data Nationality/right to work	Compliance with Employment Law Regulations Recruitment procedures SRA Code of Conduct	As part of the recruitment procedure	Stored digitally	12 months	Password protected access by directors only	Yes	Deletion from system	Legal obligation

The categories of recipients of personal data

Recipient	Why personal data provided?	Safeguards in place
Government Departments Home Office Courts HMRC Tribunals Police Health Authorities Land Registry	To progress clients matter/act on instructions	n/a as legislative and legal requirement
Experts/Interpreters/Barristers/Medical Experts, Consultants and other third party suppliers (Individuals)	To progress clients matter/act on instructions	Before instruction we will seek assurances that recipient is compliant with GDPR

Breach of Personal Data

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Any staff member who is concerned that a breach has occurred must inform the COLP. immediately.

Breaches where the ICO needs to be informed – MUST be within 72 hours of discovery

where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Individuals will be notified where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

Breach notification

The breach notification will contain:
Nature of the breach of personal data including:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned.

The name and contact details of the COLP. where more information can be obtained.

A description of the likely consequences of the personal data breach.

A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Reporting a notifiable breach

A notifiable breach has to be reported to the ICO (and also the SRA as it will be a material breach) within 72 hours of us becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows us to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, we will do so without undue delay.

Staff members must note that failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

Staff awareness

The organisation has been compliant and has ongoing compliance with the Data Protection Act, Confidentiality rules and all staff are aware and fully understand what constitutes a data breach, and that this is more than a loss of personal data.

Internal breach reporting procedure are in place for any breach situation and forms part of the Office Manual. The GDPR introduces a duty on all organisation's to report certain types of personal data breach to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible.

We will keep a record of any personal data breaches, regardless of whether we are required to notify using the form below (this will be integrated into our Central Register after the first review of this document)

Date Personal Data Breach occurred/discovered	Date reported to The COLP.	Name of staff member reporting breach	Description of breach	Has the client or any third party been affected by the breach.	How has the breach been remedied? Action taken?	Date Breach remedied	Is it a notifiable breach? If not, explanation to be given	If Notifiable Breach, date reported to the ICO	ICO Response	Action you have taken	Date of Review	Comments