DATA PROTECTION POLICY

ANNA MEDVINSKAIA

Introduction

As a Data Controller I am required to comply with the law governing the management and storage of personal data, which is outlined in the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act.

Compliance with the GDPR is overseen by the UK data protection regulator which is the Information Commissioner's Office (ICO). I am accountable to the ICO for my data protection compliance.

Purpose

This policy aims to demonstrate my compliance with the GDPR.

GDPR

The GDPR is designed to protect individuals and personal data which is held and processed about them.

The GDPR uses some key terms to refer to individuals, those processing personal data about individuals and types of data covered by the Regulation. These key terms are:

Personal data	Means any information relating to an identified and identifiable natural person ('data subject'). This includes for example information from which a person can be identified, directly or indirectly, by reference to an identifier i.e. name; ID number; location data; online identifiers etc. It also includes information that identified the physical, physiological, genetic, mental, economic, cultural or social identity of a person. For my purposes, my clients, Chambers' staff, individuals identified within my instructions and other individuals who I hold data about (such as Judges, or other barristers) are data subjects. I keep a record of the personal data that I holds in my information Asset Register.
Controller	Means the natural or legal person, public authority, agency or other body who alone or jointly with others, determines the purposes and means of processing the personal data. In effect, this means the controller is the individual, organisation or other body that decides how personal data will be collected and used. For my purposes, I am the data controller.

Processing	Means any operation which is performed on personal data such as: 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. For my purposes, everything that I do with client information (and personal information of third parties) is 'processing' as defined by the GDPR.
Special categories of personal data	Means personal data revealing: a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; d) trade-union membership; e) the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person; f) data concerning health or data concerning a natural person's sex life or sexual orientation N.B. data relating to criminal convictions and offences is not included within the special categories. However, there are additional provisions for processing this type of data (see Regulation 10 of GDPR)

Data Protection Principles

The GDPR is based around 6 principles which are the starting point to ensure compliance with the Regulation. I must adhere to these principles in performing my day-to-day duties. The principles require me to ensure that all personal data and sensitive personal data (which includes not only computer data but also personal data held within a filing system) are:

(a) Processed lawfully, fairly and in a transparent manner in relation to the subject ('lawfulness, fairness and transparency')

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

(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 ('accuracy')

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed ('storage limitation')

(f) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('integrity and confidentiality')

I must be able to demonstrate its compliance with (a) – (f) above ('accountability').

Greater protection is required for "sensitive personal data" including information held as to a person's physical or mental health, the commission of any offence and any proceedings relating to such an offence (including the outcome or sentence in such proceedings), the person's political opinions, religious or similar beliefs, sexual orientation, membership of a trade union or genetic or biometric data.

Processing personal data and sensitive personal data

I shall process all personal data in a manner that is compliant with the GDPR, in short, this means that I must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how I intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure I do not do anything unlawful with the data.

There are more restrictive provisions relating to the processing of sensitive data. The conditions for processing special categories of personal data that are most relevant to my pracitce:

- Explicit consent from the data subject (i.e. the client);
- The processing is necessary to protect the vital interests of the data subject or another person;
- The processing relates to personal data that has already been made public by the data subject; or
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

To ensure that I comply with the above principles I shall maintain and update an Information Asset Register. This shall specify as a minimum:

- The categories of personal data that I processes;
- A generalised description of the data held;
- The purpose why that data is held;
- Whether or not the data subject's consent is obtained in relation to the processing of that data, and if so how that consent is captured;
- The appropriate action of removal of consent;
- The legal basis for the processing of the personal data;
- The point where the personal data is collected;
- Where the personal data is stored;
- Whether or not the personal data is shared/published, and if so where/how. In particular whether or not the data is published to a third county or international organisation, and if so suitable safeguards.
- Whether or not the personal data is processed by a data processor, and if so who;
- The sensitivity of the personal data;
- The impact of a data breach in respect of the personal data
- The retention period/policy in respect of the data.

I shall ensure that data is processed lawfully and in accordance with GDPR. The Information Asset Register shall be reviewed by me at least every 12 months.

There are also restrictions in place for processing personal data relating to criminal convictions, which may only be carried out under official authority or where the processing is authorised by Union or Member State law. For Chambers, this means that personal data relating to criminal convictions may only be processed where this is permitted under the Data Protection Act 2018 (at the time of writing the Data Protection Bill).

For any processing that I do relating to criminal convictions I shall rely on paragraph 33 of Part 3 of Schedule 1 to the Data Protection Act 2018 as permitted processing, on the basis that it is necessary for the purpose of obtaining legal advice or for the connection with actual or prospective legal proceedings.

If I hold or write law reports I rely on the exemption in paragraph 23 of Schedule 1 to the Data Protection Act 2018.

Data accuracy

I will take reasonable steps to ensure the accuracy of personal data – "reasonable" depends on the purpose of the processing. For example I will take steps to immediately rectify any errors contained in my records.

Data collection

I shall ensure that personal data is only collected:

- Where it is necessary to do so; and
- To no greater extent than is necessary.

The Information Assert Register records how I do this.

Transparency

I shall publish a privacy notice on Chambers' website which shall set out transparently at least the following matters:

- The requirements of Articles 13 and 14 GDPR;

A reference to my privacy notice shall also accompany all instructions accepted by Chambers. For public access instructions I shall refer to my notice on any client care letter, and provide a copy along with the client care letter.

I shall review the privacy notices at least once every 12 months.

Retention of data

I shall not keep personal data for longer than is necessary. The Information Assert Register shall contain details of the retention periods for different classes of information, together with the procedures in place to ensure that such retention periods are implemented.

As part of preparation for the implementation of GDPR I have performed a data cleansing exercise and all emails over 7 years old and files containing personal information over 8 years old have been deleted or anonymised. Post GDPR I shall perform the same exercise once a year by:

- Carrying out an advanced search of my emails, using as a search term the year 7 years previously. This shall ensure that all emails for that year are captured and deleted;
- Flagging any files that contain personal data, and deleting any files over 7 years old.

As such, personal data shall not be retained on my systems for longer than 8 years, and no less than 7.

Security of data

I shall maintain a Systems Register which shall specify as a minimum:

- The system on which data is stored;
- The type of data stored;
- A description of the data;
- The security steps in place in respect of the data;
- The location of the system;
- The system owner;
- The sensitivity of the data stored;
- The impact of a data breach in respect of the personal data.

I shall review the System Register at least every 12 months.

In addition I have implemented the following procedures concerning the security of data (or paper documents)

- I shall not take any information outside of the European Union other than on a mobile telephone, laptop or other personal storage device with password protection and encryption of the data on the storage device, or through a cloud storage company (such as Drop box) which is either subject to the EU Privacy Shield or where there are other suitable security arrangements in place, which will document;
- I have a shredder in my home office for the destruction of personal information
- I shall not store documents in my home office for any sustained period of time other than when I am working on them;
- Both my work and home computer are encrypted using Mac's filevault procedure;
- All my computer and personal devices are password or pin protected, with any password involving a combination of numbers, lower case and uppercase letters at least 8 character long, and any pin being the maximum permitted by the device in question;
- Access to Dropbox requires two tier authentication;

Third party processing

I shall maintain and update the 3rd Party Register which shall specify as a minimum the name and contact details of any third party processing data on my behalf, together with the nature of the data shared with that processor. I shall ensure that all processors are subject to a written contract in place which shall include as a minimum the matters required by Article 28 GDPR.

I shall review the Third Party Register at least every 12 months.

Rights of the data subject

The GDPR gives rights to individuals in respect of the personal data that any organisations hold about them.

These rights include:

- Right of information and access to confirm details about the personal data that is being processed about them and to obtain a copy;
- Right to rectification of any inaccurate personal data;
- Right to erasure of personal data held about them (in certain circumstances);
- Right to restriction on the use of personal data held about them (in certain circumstances);
- Right to portability – right to receive data processed by automated means and have it transferred to another data controller;
- Right to object to the processing of their personal data.

I shall consider any request received from a data subject to exercise these rights and act accordingly. I shall keep a record of all decisions taken.

Where I have any concern about the identity of a person making such a request I shall take Such steps as I deem appropriate to verify that person's identity, prior to the request being actioned.

Right to information (subject access request)

Data subjects have the right to obtain from the Data Controller - confirmation as to whether or not his/her personal data is being processed; where it is; access to the personal data and the following information:

- The purposes of processing;
- The categories of personal data concerned;
- The recipients, or categories of recipients, to whom the personal data have been, or will be disclosed, including recipients in third countries or international organisations;
- Where possible, the length of time that the personal data will be stored for, or the criteria used to determine that period;
- The existence of the right to request from the Data Controller rectification or erasure of personal data or restriction of processing or to object to such processing;
- The right to lodge a complaint with the supervisory authority;
- Where personal data is not collected from the data subject, information as to the source;
- The existence of automated decision-making, including profiling, the logic involved in such decision-making and any consequences for the data subject; and
- Where personal data is transferred to a third country or international organisation, details of any safeguards in place.

Upon receipt of such a request I shall take such steps as are thought necessary to respond to the request, including where appropriate the search of emails and hard drives (including those of the clerks).

In carrying out the above function will take steps to avoid inadvertently unnecessarily processing the personal data of any third party other than the Data Subject making the subject access request.

I shall have regard to the exceptions to the right for Data Subjects to make a subject access request or the limits to such a request as set out in the Data Protection Act 2018 (at the time of writing the Data Protection Bill). In particular:

- The response must not disclose data that is subject to legal professional privilege;
- The response must not disclose information relating to another individual who can be identified from the information, unless that individual has consented or it is reasonable to disclose that information.

I shall keep a record of any response to a subject access request, including any decision I make not to disclose information as a result of an exception.

Unless otherwise requested by the Data Subject any response to a request shall be made by email, with any documents or data sent to the Data Subject being disclosed in a commonly used electronic form, such as a PDF document or a Word document.

Right to rectification of personal data

Data subjects have the right to obtain, without undue delay, the rectification of inaccurate personal data concerning them from the Data Controller.

Subject to the purposes for processing, data subjects have the right to have incomplete data completed, including by means of providing a supplementary statement.

Upon receipt of a request to correct inaccurate personal data any immediately apparent incorrect information may be corrected by the receipt of the request (for example a clerk may correct an incorrectly recorded email address) and no further action need be taken.

In the case of any request to correct inaccurate personal data that is not immediately apparent, I shall investigate as I deem appropriate. If I determine that the information is inaccurate I shall take such steps as are necessary to ensure that the incorrect data is corrected.

Save where it is apparent that it is unnecessary to do so (for example an informal request to correct an email address) I shall write to the data subject with the outcome of the request to rectify personal data.

In the event of a request to supplement incomplete data the same procedure shall be followed, save that where it is necessary to do so I shall communicate with the data subject to ascertain what information the data subject wishes to use as supplementary information. I shall then decide whether or not it is appropriate to supplement the data. I shall record any such decisions.

In the event that any request is accompanied by a request to restrict processing of data then the restriction of data procedure below shall also apply.

Erasure of personal data

Data subjects have the right to obtain from a data controller the erasure of personal data concerning them, without undue delay and the controller is obliged to erase that data where one of the following grounds applies:

- The personal data is no longer necessary in relation to the purposes for which it was collected or processed;
- The data subject withdraws the consent on which the processing is based and there is no other legal ground for processing;
- The data subject objects to the processing and there are no overriding legitimate grounds for processing;
- The personal data has been unlawfully processed;
- The personal data has to be erased for compliance with a legal obligation; or
- The personal data has been collected in relation to the offering of information society services to a child under Article 8.1. (unlikely to be applicable to Chambers)

Where the Data Controller has made the personal data public and is obliged to erase the personal data, the data controller; taking account of available technology and the cost of implementation, must take reasonable steps to inform data controllers processing the personal data that the data subject has requested erasure.

Personal data does not require to be erased where processing is necessary:

- For exercising the right of freedom of expression and information;
- For compliance with a legal obligation;
- For reasons of public interest in the area of public health Article 9.2 (h) and (i) and Article 9.3;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89.1; or
- For the establishment, exercise of defence of legal claims.

Where a request is made to erase personal data I shall take the decision as to whether (a) the data subject has the right to ask for the erasure of data; and (b) whether there is an exception

to that right that permits me to continue to retain the personal data. I shall keep a written record of all such decisions.

Without prejudice to the above decision the following circumstances would, in my opinion, still permit me to retain data notwithstanding a request for data to be erased.

- The personal data is required to be retained in order to assist with a court case. In my view it is unlikely that a data subject would have a right to request the data to be erased in these circumstances, as long as it is processed lawfully, but even if there was such a right it could be retained in the exercise of legal claims;
- The personal data is required in order to pursue a client for unpaid fees.

Restriction of processing

A data subject has the right to ask that their personal data is not processed in the following circumstances:

- They have made a request for rectification of inaccurate data or supplementation of incomplete data, in which case the data subject may ask for the processing of the data to be restricted pending the outcome of this request;
- The processing of the data is unlawful and the data subject opposed the erasure of the personal data and requests restriction instead;
- I no longer requires the personal data for processing, but it is required by the data subject for the establishment, exercise or defence of legal claims (for example the data subject wants the data retained in order to bring a claim in negligence against me, but does not want the data processed whilst it is retained)
- The data subject has objected the processing of automated decision taking (this is unlikely to apply to me).

I shall cease processing that data with the following exceptions:

- I may continue to store the personal data;
- I may continue to process the personal data to the extent that the data subject consents to such a request. This must be express consent.
- I may process the data where this involves the establishment, exercise or defence of legal claims.
- I may process personal data for the protection of the rights of another natural or legal person
- I may process the data where this is for reasons of important public interest of the European Union or of a member state.

Where a request is made to restrict the processing of personal data I shall take the decision as to whether (a) the data subject has the right to ask for processing to be restricted; and (b) whether there is an exception to that right that permits me to continue to process the personal data. I shall keep a written record of all such decisions.

Without prejudice to any decision above the following circumstances would, in my view, permit me to process data notwithstanding a request for data to be restricted.

- I may still work on a case (either pursuit of legal claims or the protection of the rights of a natural or legal person) UNLESS the client is the person who requests that the processing of data is restricted;
- I may still forward skeleton arguments or other document referring to the personal data of the data subject to the court (pursuit of legal claims).

Where the processing of data is restricted under the above procedure, and then recommences (for example if the restriction was imposed pending a determination of a request to rectify data, and that determination has not been made) then I shall inform the data subject before the restriction is lifted. This may be in writing or orally, for example via a telephone call.

Notification to third parties

Where personal data is rectified or restricted or erased under the above procedures then the I shall, unless this prove impossible or involves disproportionate effort, notify every recipient to whom the personal data has been disclosed. If the data subject requests it then I shall inform the data subject of the recipients of data.

In the event that I consider that notification would prove impossible or involve disproportionate effort I shall keep a record of this decision.

Data Portability

Data subjects have the right to receive their personal data (where they have provided it to the Data Controller), in a structured, commonly used and machine-readable format and to have the data transmitted to another data controller without hindrance, where:

- Processing is based on consent; and
- Processing is carried out by automated means.

This right is dependent on the transfer between the Data Controller and the data subject being technically feasible.
The right will not apply to processing necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.

This right cannot be exercised if it will adversely affect the rights and freedoms of others.

There are limited circumstances where consent is the legal basis of processing. Nevertheless any requests shall be considered on their merits, and I shall keep a record of this decision.

Right to Object

Data subjects have the right to object (on grounds relating to their situation) at any time to processing of their personal data which is based on:

- Necessity for the performance of a task carried out in the public interest, or in exercise of official authority vested in the Data Controller Article 6.1.e; or
- Necessity for the purposes of legitimate interests pursued by the data controller or other third party, except where this overrides the interests and fundamental freedoms of the data subject Article 6.1.f.

The Data Controller will have to stop processing the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

If personal data is processed for direct marketing purposes, data subjects can object at any time to such processing, including profiling that is related to direct marketing. Where the data subject does object, the personal data can no longer be processed for these purposes.
The right to object must be brought to the data subject's attention at the first time of communication with the data subject and should be presented clearly and separately from any other information.

I process data both on the basis that the task is in the public interest, and that there is a legitimate interest, as recorded in the Information Asset Register. In the event of a request from a data subject to cease to data being processed I shall decide whether or not there are compelling legitimate grounds to process the data. I shall keep a record of the decision reached and implement the decision, informing the data subject of the result.

In the event of a request not to have data processed for direct marketing purposes I shall immediately remove the contact details of the data subject making the request from all marketing contact lists and ensure that the clerks are also made aware of the request.

Automated Processing and Profiling

Data subjects have the right to not be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning them, or significantly affects them. This right will not apply if the decision:

- Is necessary for entering into, or performance of, a contract between the data subject and the Data Controller;
- Is authorised by Union or Member State law; or
- Is based on the data subject's explicit consent.
- The Data Controller must implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, or at least the right to obtain human intervention and contest the decision.
- Decisions referred to in paragraph 2, must not be based on special categories of data (unless the exceptions in Article 9.2 apply).

I do not take decisions based on automated processing which may significantly effect data subjects.

Time Limits

Any request to exercise the Data Subject's Rights under the GDPR must be carried out without undue delay and no later than one month from the request (which can be extended by a further two months where necessary, taking into account the complexity and number of requests).

Save for a subject access request (which I will process without undue delay but which I recognise may take up to the full month to fulfil) I will endeavour to process any other request within 7 working days of the receipt of the request.

Fees and refusal to respond

If it appears to me than any request by a Data Subject to exercise any of the above rights is manifestly unfounded or excessive, in particular because it is repetitive in character, then I shall determine:

- whether or not I should refuse to comply with the request or whether instead I should impose a reasonable administrative fee for responding to the request.
- I shall keep a record of any such decisions.

In respect of a request for further copies of data provided under a subject access request, I may decide to provide such copies or instead charge a reasonable administrative costs for complying with such a request for further copies (for example photocopying costs, if applicable). I shall keep a record of any such decision.

Other than as provided for above no charge shall be made for responding to any request by a Data Subject to exercise their rights under the GDPR.

Confidentiality And Data Sharing

I will ensure that I only shares personal information with other individuals or organisations only where I am permitted to do so in accordance with data protection law. I will comply with Chamber's Confidentiality Policy.

Wherever possible I will ensure that I have the client's (or other data subject's) consent before sharing their personal data, although, it is accepted that this will not be possible in all circumstances, for example if the disclosure is required by law.

Data Protection Officer

Article 37 GDPR requires a Data Protection Officer to be appointed in any case where:

- The processing is carried out by a public authority or body, except for courts acting in the judicial capacity.
- The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 GDPR and personal data relating to criminal convictions and offences referred to in Artile 10 GDPR.

Taking into account the nature of the Personal Data processed by me (as recorded in the Information Asset Register) and the guidance issued by the bar council I have taken the decision that it is not necessary to appoint a Data Protection Officer.

Data Protection Impact Assessments (DPIAs)

Article 35 GDPR requires DPIAs to be carried out "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

Where required, DPIAs should identify data protection risks; assess the impact of these risks; and determine appropriate action to prevent or mitigate the impact of these risks, when introducing, or making significant changes to, systems or projects involving the processing of personal data.

Taking into account the nature of scope of the data that I am likely to process (which is recorded in my information Asset Register), and having regard to the guidance issued by the Bar Council, I have taken the decision that it is not necessary for it to have carried out a DPIA in respect of my day to day data processing. However, the Information Commissioner requires a DPIA in respect of anonymous processing, which I may carry out when processing data in my instructions because the data subject may be unaware that I am processing their data. I have therefore carried out a limited DPIA in respect of this processing.

I shall keep these decisions under review, and in particular consider whether a further DPIA is required in the event of any changes to my data processing practice and procedures, and if so to require a further DPIA to be carried out. Not exhaustive examples of such changes are changes in my computing arrangements or cloud storage arrangements.

Breaches

A data protection breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Data protection breaches can happen for a wide range of reasons, including:

- Human error;
- Cyber-attacks;
- Loss or theft of devices or equipment on which personal data is stored;
- Inadequate or inappropriate access controls;
- Deceit; and
- Disasters at Chambers' premises, for example, fire or flood.

If I discover a data breach, and it is possible to do so and the timing of such action is likely to reduce or limit the effects of a data breach, I will take steps to recover any lost data and limit the data that the breach can cause.

I will then investigate the data breach, and:

- Assess the potential adverse consequences of the breach for the individuals concerned (the individuals to whom the personal data in question pertains), the potential severity or scale of the breach and the likelihood of adverse consequences occurring.
- Require such action to be taken as I view necessary to prevent a further or similar data breach from occurring in the future, including considering whether the breach is a one off incident or part of a wider systemic issue.
- Consider whether the data breach is of sufficient severity that it requires notification to the Information Commissioner, taking into account likelihood and severity of the resulting risk to people's rights and freedoms. Only in the event that I determine that it is unlikely that there is such a risk shall the breach not be notified. In assessing the risk I shall have regard to the guidance on reporting data breaches as published by the Information Commissioner, which can be found here https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.
- Consider whether the data breach should be notified to the individuals affected by the breach, taking into account whether the data breach is likely to result in a high risk to the rights and freedoms of natural persons, whether sufficient protection measures have been applied that means that the personal data is unintelligible to any person who is not authorised to access it (such as encryption), and whether such notification would involve disproportionate effort (although if notification is disproportionate I must make a public communication or a similar measure must instead be taken to ensure that data subjects are informed in an equally effective manner). In this regard it is noted the potential for a conflict arising between the obligations on me under the General Data Protection Regulation and my other legal and regulatory obligations to keep client confidentiality. I shall have regard to such conflict and take such action as is viewed appropriate, taking such guidance as is deemed necessary.

I shall keep a written record of any decisions that I take.

In the event that I determine that it is appropriate to report the breach to the Information Commissioner I shall do so without undue delay and in any event within 72 hours of becoming aware of the data breach (or if this is not possible an explanation shall be given for the delay) and the notification shall at least:

- Describe the nature of the personal data breach including where possible the categories and approximate number of data subject concerned and the categories and appropriate number of personal data records concerned.
- Communicate the name and contact details of an appropriate contact point for where more information can be obtained. This may be either me or one of the clerks.
- Describe the likely consequences of the data breach.
- Describe the measure taken or proposed to be taken to address the personal data breach, including where appropriate measures to mitigate its possible adverse effects.

To the extent that it is not possible to provide any of the above information in the initial notification this shall be provided subsequently without undue further delay.

In the event that it is determined that it is appropriate to notify individuals affected by the breach this shall be without undue delay and in a clear and plain language and contain at least the following information:

- the name and contact details of an appropriate contact point for where more information can be obtained. This shall be either me or one of the clerks.
- Details of the likely consequences of the data breach.
- Details of the measures taken or proposed to be taken to address the personal data breach, including where appropriate measures to mitigate its possible adverse effects.

Complaints

Complaints relating to breaches of the GDPR and/ or complaints that an individual's personal data is not being processed in line with the data protection principles shall be dealt with by me without undue delay.

Penalties

It is important that I understand the implications if I fail to meet my data protection obligations. Failure to comply could result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- Suspension/ withdrawal of the right to process personal data by the ICO;

- Loss of confidence in the integrity of the business's systems and procedures;
- Irreparable damage to the business's reputation.

Note: I could be fined up to €20,000,000, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.