Company Name	**A1 Locums**
Document	**General Data Protection Regulation (GDPR)**
Topic	**Data Protection**
Date	**17th May 2018**
Version	**2**

Contents:

Introduction

A1 Locums has been operating for 14 years and is an introductory agency which means that we do not pay anyone, but we charge the practices a daily fee, each time we place a locum with them. Our service is free of charge to our locums and the practice will be responsible for paying its own locums.

As part of our compliance with GDPR, we would like to tell you how we store and manage your personal data.

In this policy the following terms have the following meanings:

'*consent*' means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of persona data relating to him or her.

'*data controller*' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*.

'*data processor*' means an individual or organisation which processes *personal data* on behalf of the *data controller*.

'*personal data*'* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'*personal data breach*' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data*.

'*processing*' means any operation or set of operations performed on *personal data*, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'*profiling*' means any form of automated *processing* of *personal data* consisting of the use of *personal data* to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

'*pseudonymisation*' means the *processing* of *personal data* in such a manner that the *personal data* can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the *personal data* are not attributed to an identified or identifiable individual.

'*sensitive personal data*'* means *personal data* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the *processing* of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions. [Note 1]

* For the purposes of this policy we use the term '*personal data*' to include '*sensitive personal data*' except where we need to refer to *sensitive personal data* specifically.

'*supervisory authority*' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is the Information Commissioner's Office (ICO).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

General Data Protection regulation (GDPR) policy:

The Company processes *personal data* in relation to its own staff, work-seekers and individual client contacts and is a *data controller* for the purposes of the Data Protection Laws. The Company has registered with the ICO and its registration number is **Z2898907**

The Company may hold *personal data* on individuals for the following purposes:

- Staff administration;
- Advertising, marketing and public relations.
- Accounts and records;
- Administration and *processing* of veterinary professional's *personal data* for the purposes of providing work-finding services, including *processing* using software solution providers and back office support
- Administration and *processing* of clients' *personal data* for the purposes of supplying/introducing veterinary professionals.
- Providing umbrella companies with personal data.

The Company will only process *personal data* where it has a legal basis for doing so. Where the Company does not have a legal reason for *processing personal data* any *processing* will be a breach of the Data Protection Laws.

Information Security

Only those listed in the Appendix are permitted to add, amend or delete personal data from the Company's database(s) ('database' includes paper records or records stored electronically).

All Company staff are responsible for notifying those listed in the Appendix where information is known to be old, inaccurate or out of date or a request for erasure, access, rectification or restriction of processing has been received from the individual. Company staff are also responsible for notifying those listed in the Appendix where any request for data portability, objection to processing or where consent to process has been withdrawn and has been received from the individual.

The incorrect processing of personal data e.g. sending an individual's details to the wrong person, allowing unauthorised persons access to personal data, sending information out for purposes for which the individual did not give their consent, or not having a lawful reason to process personal data, may give rise to a breach of contract and/or negligence leading to a claim against the Company for damages from an employee, work-seeker or client contact.

In addition, all Company staff should ensure that adequate security measures are in place to limit the risk of personal data breaches. For example:

- Staff should lock their computer screens when they are not in use.
- All devices, whether company or personal devices (including but not limited to computers, mobile phones, other hand-held devices) containing personal data relating to the services of the Company shall be encrypted and password protected. OR All personal data collected via a company or personal device for the purposes of providing the Company's services, should be processed through the Company's CRM.
- Staff should not disclose their passwords to anyone.
- Email should be used with care. Company staff must ensure that emails are sent only to the intended recipient/s. Where Company staff send an email in error then the email must be recalled immediately, and Company staff must inform those listed in the Appendix of the error so that any risk of a personal data breach can be limited.
- Personnel files (whether for internal staff or work-seekers) and other personal data should be stored securely to prevent unauthorised access. They should not be removed from their usual place of storage without good reason.
- Personnel files (whether for internal staff or work-seekers) should always be locked away when not in use and when in use should not be left unattended.
- Personal data should only be stored for the periods set out in the Company's data retention policy.
- Processing includes the destruction or disposal of personal data. Therefore, staff should take care to destroy or dispose of personal data safely and securely. Such material should be shredded or stored as confidential waste awaiting safe destruction.

Rights of the individual.

An individual has the following rights under the Data Protection Laws:

1. The right to be informed of what information the Company holds on them – this is typically given to the individual in a privacy notice;
2. The right of access to any personal data that the Company holds on them – this is usually referred to as a 'subject access request';
3. The right to rectification of personal data that the individual believes is either inaccurate or incomplete;
4. The right to erasure of their personal data in certain circumstances;
5. The right to restrict processing of their personal data;
6. The right to data portability of their personal data in specific circumstances;

7. The right to object to the processing of their personal data where it is based on either a legitimate interest or a public interest;

8. The right not to be subjected to automated decision making and profiling; and

9. The right to withdraw consent where it was relied upon to process their personal data.

In order for consent to be valid it must be:

- Freely given:
- Specific
- Informed
- Unambiguous
- It must be as easy to withdraw as it is to give consent.

How your data is processed by A1 Locums

Your profiles are held on our data base, which is securely held in the cloud. Your CV is held against your profile and is then watermarked, and your personal details, i.e. residential address, telephone and email are removed.

Other personal data such as Passport, Visas, Competency skills, Information questionnaire are all held in a secure file on our server and is only accessed by recruiters and administrators.

Your CV will not be forwarded to any employers without your prior consent, in writing via email. We will also not share your personal information with any third party i.e. an umbrella company, without prior written consent.

Registering with A1 Locums

Once you have registered with us via our website or via our office, we will keep your data in pre-registered until we have received all your relevant information to allow you to work with A1 Locums. We will contact you three times for the information and if we do not receive it, then we will delete this information from our system.

Once we have received all your information, you will go into our registered database and we will then be able to contact you with suitable vacancies. You will be included in our bulk email, if you request us to include you and will have the option at any time to:

- Unsubscribe to bulk emails or texts.
- Become in-active (short-term removal, i.e. In a permanent job, travelling overseas and maternity cover)
- Delete permanently (retired, out of the industry or no longer want to deal with A1 Locums.

What is the legitimate interests condition?

This is of particular interest to recruitment companies, as they have an interest in processing personal data. Recruiters provide work finding services for both candidates and clients. They provide personal data in order to be able to provide these services, they need to check identity, right to work as well as process pay and manage entitlement to certain statutory rights

We may have to process this for A1 Locums or for those third parties to whom we may have to disclose information. The processing of this information must be fair and lawful and must comply with all the data protection principles.

1 Right to be informed

Any individual whose personal data is processed by the Company will have the right to be informed about such processing. They will have the right to be informed about who, what, where and why the data is processed. This information should be delivered in a privacy notice, in writing and where appropriate electronically. Depending on where the personal data are being collected, an individual may be directed to the Company's website privacy notice or be given a copy of a privacy notice. This privacy notice should be issued in instances where either:

a) the Company collects/processes data directly from the individual; or

b) the Company has not collected/processed the data from the individual directly.

In addition:

a) Where personal data has been collected from the individual the privacy notice will need to be issued at the point the data is collected. Where the Company intends to further process the personal data for a purpose other than that for which the personal data was collected, the Company shall provide the individual, prior to that further processing, with information on that other purpose and with any relevant further information in [a new/an] updated privacy notice.

b) Where personal data has not been obtained from the individual, the Company shall provide the privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed. If the personal data are to be used to communicate with the individual, then the privacy notice will be issued at the time of the first communication with the individual. If a disclosure to another recipient is envisaged, then the privacy notice will be issued to the individual at the latest when the personal data are first disclosed.

2.The right to access (subject access request)

Individuals are entitled to obtain access to their personal data on request, free of charge except in certain circumstances.

An individual will be entitled to the following information:

- Confirmation that their personal data is or is not being processed;
- Access to the personal data undergoing processing;
- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, recipients in third countries or international organisations;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the Company rectification or erasure of personal data or restriction of processing of personal data concerning the individual or to object to such processing;
- The right to lodge a complaint with the ICO or any other relevant supervisory authority;
- Where the personal data are not collected from an individual, any available information as to the source of that information;
- The existence of automated decision-making, including profiling, based on a public interest or a legitimate interest and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

If the Company transfers the individual's personal data to a third country or to an international organisation, the individual shall have the right to be informed of the appropriate safeguards in place relating to the transfer.

If the Company processes a large quantity of information concerning the individual making the request, the Company might request that the individual specify the information or processing activities to which the request relates to specifically before the information is delivered. If such a

request is required by the Company then it shall be delivered promptly to the individual, taking into consideration the timeframes within which the subject access requests must be completed.

The individual's right to access their information shall not adversely affect the rights and freedoms of others and they will not be able to access the personal data of third parties without the explicit consent of that third party or if it is reasonable in all the circumstances to comply with the request without that third party's consent, taking into consideration any means to redact the personal data of any third party. Persons listed in the Appendix will decide whether it is appropriate to disclose the information to the individual on a case by case basis. This decision will involve balancing the individual's right of access of their personal data against the third party's rights in respect of their own personal data.

Note: An individual may not label their subject access request as such. Therefore, Company staff should always consider whether a request is a subject request even when not called that. If in doubt, check with Clare Alderton, Data Controller.

3. The right to rectification

An individual, or another data controller acting on an individual's behalf, has the right to obtain from the Company rectification of inaccurate or incomplete personal data concerning him or her. The Company must act on this request without undue delay.

Taking into account the purposes of the processing, the individual shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement stating what they would require to be completed.

The Company shall communicate any rectification of personal data to each recipient to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort. The Company shall inform the individual about those recipients if he or she requests it.

Where the Company, acting as a data processor, receives information from a data controller to rectify an individual's personal data, then the Company shall comply with this request unless this proves impossible or involves disproportionate effort.

In circumstances where the Company is unable to comply with the request as it proves impossible or involves disproportionate effort, the Company will document this in a privacy impact assessment or similar.

4. The right to erasure ('right to be forgotten')

An individual shall have the right to obtain from the Company, acting as data controller, the erasure of personal data concerning him or her without undue delay. The Company will be obliged to erase the individual's personal data without undue delay where one of the following grounds apply:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- An individual withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
- An individual object to the processing (based on either a public interest or a legitimate interest) and there are no overriding legitimate grounds for the processing, or an individual objects to the processing for direct marketing purposes (including profiling related to direct marketing);
- The personal data have been unlawfully processed;
- The personal data must be erased for compliance with a legal obligation; or
- The personal data have been collected in relation to the offer of information society services to a child.

Where the Company, acting as data controller, has made the personal data public and is obliged to erase that personal data, the Company, taking into account available technology and the cost of implementation, shall take reasonable steps, including technological measures, to inform data processors who are processing the personal data that an individual has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The Company will not be obliged to erase information to the extent that processing is necessary:

- For exercising the right of freedom of expression and information;
- For compliance with a legal obligation which requires processing, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company acting as controller;
- For reasons of public interest in the area of public health;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- For the establishment, exercise or defence of legal claims.

The Company shall communicate any erasure of personal data to each recipient to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort. The Company shall inform the individual about those recipients if an individual request it.

Where the Company, acting as a data processor, receives information from a data controller to erase an individual's personal data the Company shall comply with this request, unless this proves impossible or involves disproportionate effort.

In circumstances where the Company is unable to comply with the request as it proves impossible or involves disproportionate effort, the Company will document this in a privacy impact assessment or similar.

5. The right to restrict processing

An individual will have the right to obtain from the Company, acting as a data controller, the restriction of processing his or her personal data where one of the following applies:

- The accuracy of the personal data is contested by the individual, for a period enabling the Company to verify the accuracy of the personal data;
- The processing is unlawful, and the individual opposes the erasure of the personal data and requests the restriction of their use instead;
- The Company no longer needs the personal data for the purposes of the processing, but they are required by an individual for the establishment, exercise or defence of legal claims;
- The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the individual's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

Where an individual has successfully asked for their personal data to be restricted, then the Company will inform the individual before such a restriction is lifted.

The Company shall communicate any restriction of processing to each recipient to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort. The Company shall inform the individual about those recipients if he or she requests it.

Where the Company, acting as a data processor, receives information from a data controller to restrict processing an individual's personal data, the Company shall comply with this request, unless this proves impossible or involves disproportionate effort.

In circumstances where the Company is unable to comply with the request as it proves impossible or involves disproportionate effort, the Company will document this in a privacy impact assessment or similar.

6. The right to data portability

An individual has the right to receive any personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data controller where:

- The processing is based on the individual's consent or a contract; and
- The processing is carried out by automated means.

Company staff will advise those listed in the Appendix when they receive a request to port data. Those listed in the Appendix will be responsible for identifying if the above circumstances are satisfied for the purposes of porting the data to the individual and/or another data controller.

For the avoidance of doubt, there is no obligation to port personal data that is not kept by automated means by the Company.

7. The right to object to processing

An individual, has the right to object to their personal data being processed or profiled based on a public interest or a legitimate interest.

Where the Company receives an objection to processing or profiling on the above, those listed in the Appendix will ensure that the processing and/or profiling ceases unless such persons can establish compelling grounds to continue to process the personal data. If this is the case those persons listed in the Appendix will document this in a privacy impact assessment or similar**.**

8. Automated decision making

An individual has the right not to be subjected to an automated decision-making process, including profiling, that produces a legal effect or a similarly significant effect on the individual. The Company does not use such automated decision-making processes except in the following exceptional circumstances.

It is possible to subject an individual to automated decision making processes, including profiling, where:

a) It is necessary for entering into or performance of a contract between the employer and the individual;

b) It is authorised by law; or

c) The individual has given their explicit consent.

Where a) and c) apply the Company will ensure that suitable measures are in place to safeguard the individual's rights and freedoms and legitimate interests, under both Data Protection Laws and the Human Rights Act 1998, before this type of processing occurs for personal data.

Where a) to c) apply the Company will only process sensitive personal data where the Company has received either the explicit consent to do so or there is a substantial public interest to do so. Again, the Company will ensure that suitable measures are in place to safeguard the individual's rights and freedoms and legitimate interests, under both Data Protection Laws and the Human Rights Act 1998, before this type of processing occurs for sensitive personal data.

The safeguarding measures include:

- Conducting a risk assessment as to what risks are posed to the individual's rights and freedoms;
- Ensuring where the automated decision-making process is necessary for entering into or performance of a contract, that this is documented clearly by the Company;
- Ensuring where explicit consent is given this is documented clearly by the Company

9. The right to withdraw consent

Where the Company relies on an individual's consent to process their personal data then the Company will advise the individual that they have the right to withdraw his or her consent at any time.

Any Company staff who receive a request from an individual to withdraw their consent to processing their data will be responsible for issuing the individual with the Company's withdrawal of consent form. Once the form has been completed it should be given to the persons listed in the Appendix to process the individual's request further.

If an applicant requests that they want all their data sent to another recruitment company or to themselves, we will arrange for all this data to be put into a CSV file and for this to be forwarded to them within 28 days (unless we stipulate why the information cannot be processed, i.e. invoicing or still working for us.

10. Timing and information to be provided to the individuals

The Company shall provide information on action taken or not taken with regard to the individual data protection rights, set out in paragraphs 1 to 9 inclusive, without undue delay and in any event within one month of receipt of the request. Where the Company does take action, then it may, where necessary, extend this period by a further two months, taking into account the complexity and number of the requests. Those persons listed in the Appendix shall inform an individual of any extension within one month of receipt of the request, together with the reasons for the delay. Where the Company does not take action on the request of the individual then those persons listed in the Appendix will inform him or her of the possibility of lodging a complaint with the Information Commissioner's Office (ICO) and seeking a judicial remedy.

11. Charges

Where requests from an individual are manifestly unfounded or excessive, in particular because of their repetitive character, the Company may either:

- Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- Refuse to act on the request.

The Company must demonstrate whether the request is manifestly unfounded or excessive. Those listed in the Appendix will be responsible for demonstrating this.

Where the individual makes the request by electronic means the Company shall provide the information in a commonly used electronic form, unless otherwise requested by the individual.

The Company will need to act on any personal data protection breach it suspects or knows of when acting as either a data controller or a data processor.

Company staff must inform those persons listed in the Appendix where a personal data breach has either been reported to him or her or they themselves have identified a personal data breach.

1. Personal data breaches where the Company is the data controller:

Those listed in the Appendix will take measures to establish whether or not a personal data breach has occurred. Those persons will:

- Conduct a risk assessment as to what level of risk the personal data breach poses/has occurred;
- Conduct any relevant interviews or investigations of the Company's practices and/or Company staff to assess how the personal data breach occurred
- Implement measures and take steps to limit, contain and recover the breach

Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual, then those listed in the Appendix will be responsible for alerting the ICO of any personal data breach without undue delay, but no later than 72 hours after having become aware of the Company's personal data breach. Where it is not possible to inform the ICO in this time those listed in the Appendix will be responsible for explaining to the ICO the reasons for the delay.

If the personal data breach happens outside the UK then those listed in the Appendix will be responsible for alerting the relevant supervisory authority in the affected jurisdiction.

If those listed in the Appendix are not able to provide the ICO/other relevant supervisory authority with all the relevant information related to the personal data breach then those persons shall provide the information in phases without undue further delay.

Those listed in the Appendix will be responsible for documenting any personal data breaches, including:

- The facts relating to the personal data breach – including any investigations undertaken or statements taken from the Company's staff;
- The effects of the personal data breach; and
- The remedial action taken.

2. Personal data breaches where the Company is the data processor:

Those listed in the Appendix will be responsible for alerting the relevant data controller as to the personal data breach that has been identified as soon as they are aware of the breach, having particular regard to any contractual obligations the Company has with the data controller.

3. Communicating personal data breaches to individuals

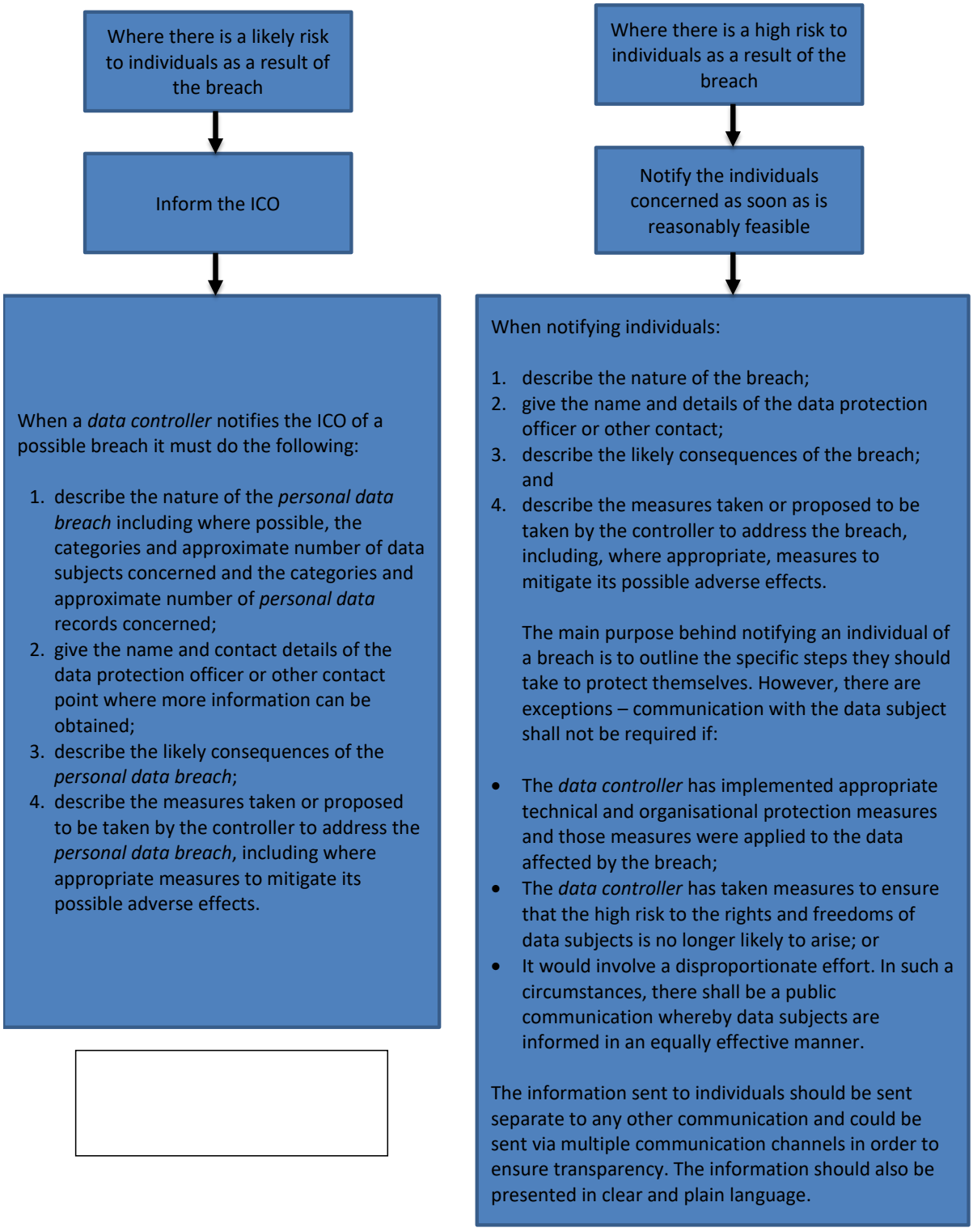
Where a personal data breach has been identified, which results in a high risk to the rights and freedoms of individuals, those listed in the Appendix will be responsible for informing those individuals effected by the personal data breach without undue delay.

A1 Locums will have the right to not be able to complete erasure in 1 month where a locum is still within a 6-month contract with a practice, or where there is invoicing outstanding for ongoing work.

A1 Locums will notify the ICO of any personal data breaches no later than 72 hours after the time they are made aware of it.

The data protection measures and this policy will be reviewed on an annual basis.

Actions to take after a breach



General Data Protection regulation (GDPR) policy:

Those listed in the Appendix will keep written records of the processing activities of the Company. The records must be in writing (which can be in electronic form) and must include the following information:

- The name and contact details of the data controller or data controller's representative and any joint controllers;
- The purposes of the processing;
- A description of the categories of the data subjects and of the categories of the personal data;
- The categories of recipients to whom personal data have or will be disclosed to, including to those internationally;
- Any transfers of personal data internationally, including the identification of the third country or international organisation to which the data is transferred;
- The envisaged time limits placed on an individual's right to erasure; and
- Where possible, a description of the technical and security measures that have been utilised to alleviate data-related risks.

The Company will also document:

- Information required for privacy notices;
- Records of consent;
- Controller-processor contracts;
- The location of personal data;
- Data Protection Impact Assessment reports;
- Records of personal data breaches;
- Information required for processing sensitive personal data or criminal convictions/offences data.

The Company will make these records available to the ICO upon request.

A1 Locums will review this policy and update it on a regular basis.

Appendix

Responsibilities held within the Company:

Data Controller: Clare Alderton (Owner and MD)

- Setting out of purposes for which and manner in which any personal data is to be processed
- Reporting data breaches/dealing with complaints
- Informing and advising the organisation
- Monitoring compliance
- Co-operating with supervisory authority and acting as first point of contact

Data Processor:

- Adding, amending data on behalf of the Data Processor: **Recruitment Team and Recruitment administrators**
- Deleting personal data: **Data Processor.**
- Responding to subject access requests/requests for rectification, erasure, restriction data portability, objection, automated decision-making processes and profiling and withdrawal of consent **Data Processor.**