

# VIRIDIAN Data Protection Policy

Version No:	1.0
Version Date:	October 2021
Approval Date:	21 October 2021
Approved By:	Director
Policy Document No:	TBA

## 1. INTRODUCTION AND PURPOSE

- 1.1. This policy sets out the data protection obligations of Alexandra Fraser Consulting Ltd (Pty) trading as Viridian, a company registered in the Republic of South Africa under registration number 2016/098527/07, whose registered office is at 10 Ash Street, Observatory, Cape Town ("**VIRIDIAN**") ("**Policy**").
- 1.2. In particular, this Policy summarises how VIRIDIAN processes personal data belonging to, amongst others, its staff, business contacts, beneficiaries, funders, donors, suppliers, and programme participants ("**data subjects**").
- 1.3. VIRIDIAN takes the privacy of personal data very seriously, and is committed to processing personal data in accordance with data protection legislation, including, where applicable, the General Data Protection Regulation (EU 2016/679), the retained EU law version of the General Data Protection Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland, and Northern Ireland (together, "**GDPR**"), the Protection of Personal Information Act (No. 4 of 2013) ("**POPI**"), and any other applicable data protection legislation and/or regulation in force from time to time ("**Data Protection Laws**").

## 2. DEFINITIONS

- 2.1 In this Policy, the following words mean:
  - 2.1.1 **AEEI**. African Entrepreneurship Ecosystem Investors (AEEI), a non-profit company registered in the Republic of South Africa under registration number 2021/593658/08
  - 2.1.2 **consent**. The consent of a data subject, which consent must be a freely given, specific, informed, and unambiguous indication of the relevant data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.
  - 2.1.3 **data controller**. The natural or juristic person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- 2.1.4 **data processor.** A natural or juristic person who processes personal data on behalf of a data controller.
  - 2.1.5 **Data Protection Officer.** As contemplated in GDPR.
  - 2.1.6 **personal data.** Any information relating to a data subject who can be identified, directly or indirectly, by reference to an identifier such as a name, 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 data subject.
  - 2.1.7 **personal data breach.** 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.
  - 2.1.8 **processing.** Any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, 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.
  - 2.1.9 **anonymisation.** The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject 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 is not attributed to an identified or identifiable natural person.
  - 2.1.10 **special category personal data.** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, political persuasion, health, sexual life, sexual orientation, biometric, genetic data, or criminal sanctions.
  - 2.1.11 **Viridian.** Alexandra Fraser Consulting Proprietary Limited t/a Viridian (Registration No. 2016/098527/07).
- 2.2 In this Policy:
- 2.2.1 The words "**include**", "**including**" and "**in particular**" are by way of example only and shall not limit the generality of any preceding words.
  - 2.2.2 if any provision becomes illegal, invalid or unenforceable, such provision shall be severed, to the extent of its illegality, invalidity or unenforceability, from the balance of this agreement; and
  - 2.2.3 the words "**other**" and "**otherwise**" shall be interpreted as widely as possible and will not be limited by any preceding words.
- 2.3 This Policy has largely been drafted using the terminology contemplated in GDPR. Where this Policy is interpreted in the context of POPI, the terms:
- 2.3.1 "**Data Protection Officer**" shall be read as "**Information Officer**";
  - 2.3.2 "**data controller**" shall be read as "**responsible party**";

2.3.3 "**personal data**" shall be read as "**personal information**"; and

2.3.4 "**special category personal data**" shall be read as "**special personal information**",

as those terms are defined in POPI.

### **3. SCOPE**

The procedures and principles set out in this Policy must be followed at all times by VIRIDIAN, its employees, agents, contractors, and other parties working on behalf of VIRIDIAN, including third-party data processors processing personal data on VIRIDIAN's behalf.

### **4. DATA PROTECTION OFFICER**

4.1 VIRIDIAN's Data Protection Officer is **Alexandra Fraser, Director (alex@viridian.africa)**  
The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

4.2 The Data Protection Officer, in collaboration with VIRIDIAN's board of directors, is responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of VIRIDIAN comply with this Policy and, where applicable, implement all such practices, processes, controls, and training as is reasonably necessary to ensure such compliance.

4.3 Any questions relating to this Policy or to Data Protection Laws should be referred to VIRIDIAN's Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

4.3.1 if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;

4.3.2 if consent is being relied upon in order to collect, hold, and/or process personal data;

4.3.3 if there is any uncertainty relating to the retention period for any particular type(s) of personal data;

4.3.4 if any new or amended privacy notices or similar privacy-related documentation are required;

4.3.5 if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of a subject's request/s);

4.3.6 if a personal data breach (whether suspected or actual) has occurred;

4.3.7 if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;

4.3.8 if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

- 4.3.9 if personal data is to be transferred outside of the country in which it is originally processed and there are questions relating to the legal basis on which to do so;
- 4.3.10 when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a data protection impact assessment to identify and minimise the data protection risks associated with a particular project;
- 4.3.11 when personal data is to be used for purposes different to those for which it was originally collected;
- 4.3.12 if any automated processing, including profiling or automated decision-making, is to be carried out; or
- 4.3.13 if any assistance is required in complying with the law applicable to direct marketing.

## **5. THE RIGHTS OF DATA SUBJECTS**

- 5.1 VIRIDIAN is committed to upholding the rights of data subjects, which rights include:
  - 5.1.1 the right to be informed;
  - 5.1.2 the right of access;
  - 5.1.3 the right to rectification;
  - 5.1.4 the right to erasure (also known as *the right to be forgotten*);
  - 5.1.5 the right to restrict processing;
  - 5.1.6 the right to data portability;
  - 5.1.7 the right to object; and
  - 5.1.8 rights with respect to automated decision-making and profiling.

## **6. DATA PROTECTION PRINCIPLES**

VIRIDIAN is committed to processing personal data only in a manner that:

- 6.1 is lawful, fair, and transparent;
- 6.2 is specified, explicit, and legitimate, and for a particular purpose. VIRIDIAN will not further process personal data in a manner that is incompatible with the initial purpose for which the personal data was obtained. Further processing for archiving purposes in the public interest, or research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- 6.3 is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- 6.4 is accurate. VIRIDIAN takes reasonable steps to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or

rectified without delay;

- 6.5 permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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, or research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by Data Protection Law in order to safeguard the rights and freedoms of the data subject; and
- 6.6 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.

## **7. PERSONAL DATA**

The personal data processed by VIRIDIAN includes:

### **7.1 Suppliers:**

company registration numbers (in the case of juristic persons), identity numbers (in the case of natural persons), physical addresses, value-added-tax numbers, phone numbers, email addresses, bank details, and, in certain circumstances, information relating to the data subject's race and/or gender;

### **7.2 Funding partners/clients:**

company registration numbers (in the case of juristic persons), identity numbers (in the case of natural persons), physical addresses, value-added-tax numbers, phone numbers, email addresses, bank details;

### **7.3 Employees and consultants:**

identity numbers, income tax number, address, phone and email, race and gender, and any other information voluntarily provided by a data subject pursuant to that data subject application for employment with VIRIDIAN; and

### **7.4 Programme participants:**

VIRIDIAN collects personal data belonging to those data subjects who have participated or applied to participate in a VIRIDIAN programme for hubs and/or early-stage entrepreneurs and/or investors. This personal data is collected through forms, surveys and other voluntary means, and relates to, amongst other things, the data subject's business, existing skills, and how the participant is progressing with the skills that have been obtained through the relevant programme.

## **8. LAWFUL, FAIR, AND TRANSPARENT DATA PROCESSING**

- 8.1 Data Protection Laws seek to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. VIRIDIAN shall only process personal data if at least one of the following apply:

- 8.1.1 the data subject has given consent to the processing of their personal data for one or more specific purposes;
  - 8.1.2 the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
  - 8.1.3 the processing is necessary for compliance with a legal obligation to which the data controller is subject;
  - 8.1.4 the processing is necessary to protect the vital interests of the data subject or of another natural person;
  - 8.1.5 the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; and/or
  - 8.1.6 processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- 8.2 The processing of sensitive personal data or a special category of personal data shall be lawful if at least one of the following applies:
- 8.2.1 the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);
  - 8.2.2 the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
  - 8.2.3 the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
  - 8.2.4 the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
  - 8.2.5 the processing relates to personal data which is manifestly made public by the data subject;
  - 8.2.6 the processing is necessary for the conduct of legal claims or whenever courts

are acting in their judicial capacity;

- 8.2.7 the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- 8.2.8 the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in GDPR;
- 8.2.9 the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- 8.9.10 the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with GDPR, based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

## **9. CONSENT**

Where VIRIDIAN relies on consent as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

- 9.1 consent shall only be deemed to be granted by a data subject where it is obtained in the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity will not be regarded as amounting to consent;
- 9.2 where consent is given in a document which includes other matters, the section dealing with consent will be kept clearly separated from such other matters;
- 9.3 data subjects will always be free to withdraw their consent at any time;
- 9.4 where VIRIDIAN intends processing personal data for a different purpose (that is incompatible with the purpose for which that personal data was originally collected), VIRIDIAN will obtain further consent of the relevant data subject.
- 9.5 where VIRIDIAN processes special categories of personal data, it generally does so with a lawful basis. However, if explicit consent is relied upon for any such processing by VIRIDIAN, the data subject in question must be issued with a suitable privacy notice in order to capture their consent;
- 9.6 VIRIDIAN shall not knowingly process the personal data belonging to a child under the age of 18, unless it obtains the consent from a person who is legally competent to

consent to any action or decision being taken in respect of that child; and

9.7 records shall be kept in respect of all consents obtained by VIRIDIAN for the processing of personal data.

## **10. SPECIFIED, EXPLICIT, AND LEGITIMATE PURPOSES**

VIRIDIAN only collects, processes, and holds personal data for the specific purposes set out in this Policy.

## **11. ADEQUATE, RELEVANT, AND LIMITED DATA PROCESSING**

11.1 VIRIDIAN will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed.

11.2 Employees, agents, contractors, or other parties working on behalf of VIRIDIAN shall:

11.2.1 collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy; and

11.2.2 process personal data only when the performance of their job duties requires it.

## **12. ACCURACY OF DATA**

12.1 VIRIDIAN shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date.

12.2 If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken by VIRIDIAN without delay to amend or erase that data, as appropriate.

## **13. DATA STORAGE AND RETENTION**

13.1 Personal data, is stored by VIRIDIAN in the following ways and in the following locations:

13.1.1 VIRIDIAN's own servers, located in the Google Cloud and G Drive, with global locations;

13.1.2 third-party servers, operated by Airtable and located in the United States;

13.1.3 computers permanently located at VIRIDIAN's business premises;

13.1.4 laptop computers and other mobile devices provided by VIRIDIAN to its employees;

13.1.5 computers and mobile devices owned by employees, agents, and sub-contractors; and

13.1.6 physical records stored at VIRIDIAN's premises.

13.2 VIRIDIAN shall not keep personal data for any longer than is necessary in light of the purpose for which that personal data was originally collected, held, and processed.

- 13.3 When personal data is no longer required, it will either be anonymised, or all reasonable steps will be taken to erase or otherwise dispose of it without delay.

## **14. SECURE PROCESSING**

- 14.1 VIRIDIAN shall ensure that all personal data collected, held, and processed by it is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- 14.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.
- 14.3 VIRIDIAN will adhere to the following guidelines to protect against the confidentiality, integrity, and availability of all personal data:
- 14.3.1 only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;
  - 14.3.2 personal data must be accurate and suitable for the purpose for which it is collected, held, and processed; and
  - 14.3.3 authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

## **15. ACCOUNTABILITY AND RECORD-KEEPING**

- 15.1 A data protection impact assessment shall be conducted if any processing of personal data presents a significant risk to the rights and freedoms of data subjects.
- 15.2 All employees, agents, contractors, or other parties working on behalf of VIRIDIAN shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Laws, this Policy, and all other applicable VIRIDIAN policies.
- 15.3 VIRIDIAN's data protection compliance shall be regularly reviewed and evaluated by the Data Protection Officer.
- 15.4 VIRIDIAN will keep adequate internal records in respect of the processing of personal data.

## **16. DATA SUBJECT ACCESS**

- 16.1 Data subjects may, at any time, request the Data Protection Officer to supply details as to the personal data which VIRIDIAN holds about that data subject, what VIRIDIAN is doing with that personal data, and why.
- 16.2 VIRIDIAN does not charge a fee for the handling of normal requests. However, VIRIDIAN reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.
- 16.3 Data Subject Access Request Forms can be accessed here <https://bit.ly/3iHpf0f>

## **17. RECTIFICATION OF PERSONAL DATA**

- 17.1 Data subjects have the right to require VIRIDIAN to rectify any of their personal data that is inaccurate or incomplete. VIRIDIAN shall comply with such requests timeously.
- 17.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

## **18. ERASURE OF PERSONAL DATA**

- 18.1 Data subjects have the right to request that VIRIDIAN erases the personal data it holds about them in certain circumstances, for example, where the data subject withdraws its consent for the processing of its personal data.
- 18.2 Unless VIRIDIAN has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with timeously, and the data subject informed of the erasure.
- 18.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

## **19. RESTRICTION OF PERSONAL DATA PROCESSING**

- 19.1 Data subjects may request that VIRIDIAN ceases processing the personal data it holds about them. If a data subject makes such a request, VIRIDIAN shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
- 19.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

## **20. DATA PORTABILITY**

Data subjects have the right to receive a copy of their personal data in VIRIDIAN's possession in a structured, commonly used and machine readable format, and to request its transmission to another data controller.

## **21. OBJECTIONS TO PERSONAL DATA PROCESSING**

- 21.1 Data subjects have the right to object to VIRIDIAN processing their personal data based on legitimate interests, for direct marketing (including profiling), and processing for research and statistics purposes.
- 22.2 Where a data subject objects to VIRIDIAN processing their personal data based on its legitimate interests, VIRIDIAN shall cease such processing immediately, unless it can be demonstrated that VIRIDIAN's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the

conduct of legal claims.

22.3 Where a data subject objects to VIRIDIAN processing their personal data for direct marketing purposes, VIRIDIAN shall cease such processing promptly.

22.4 Where a data subject objects to VIRIDIAN processing their personal data for research and statistics purposes, the data subject must demonstrate grounds relating to his or her particular situation. VIRIDIAN is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

## **23. DIRECT MARKETING**

23.1 VIRIDIAN shall obtain a data subject's prior consent for direct marketing including email, text messaging, and automated telephone calls.

23.2 If a data subject objects to direct marketing, VIRIDIAN shall comply with the request promptly.

## **24. TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES**

24.1 Where possible, the following technical measures shall be implemented within VIRIDIAN to protect the security of personal data:

24.1.1 emails containing personal data must be marked "confidential";

24.1.2 personal data is only transmitted over secure networks;

24.1.3 personal data is not transmitted over a wireless network if there is a reasonable wired alternative;

24.1.4 all personal data transferred physically should be transferred in a suitable container and marked "confidential";

24.1.5 no personal data shall be shared informally, and if access is required to any personal data, such access should be formally requested;

24.1.6 all hardcopies of personal data, along with any electronic copies stored on physical media shall be stored securely;

24.1.7 no personal data shall be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of VIRIDIAN or not, without authorisation;

24.1.8 personal data shall be handled with care at all times and should not be left unattended or on view;

24.1.9 all electronic copies of personal data shall be stored securely using passwords;

24.1.10 all passwords used to protect personal data shall be changed regularly;

24.1.11 no passwords shall be written down or shared. If a password is forgotten, it must be reset using the applicable method; and

24.1.12 no unauthorised software may be installed on any VIRIDIAN-owned computer or device without prior written approval from the Data Protection Officer.

24.2 Where possible, the following organisational measures shall be implemented within VIRIDIAN to protect the security of personal data:

24.2.1 all employees and other parties working on behalf of VIRIDIAN shall be made fully aware of both their individual responsibilities and VIRIDIAN's responsibilities under the Data Protection Laws and this Policy and shall be bound to comply with the Data Protection Laws and this Policy;

24.2.2 only employees and other parties working on behalf of VIRIDIAN that need access to, and use of, personal data in order to perform their work shall have access to personal data held by VIRIDIAN;

24.2.3 all employees and other parties handling personal data on behalf of VIRIDIAN will be appropriately trained to do so and shall exercise care and caution when discussing any work relating to personal data at all times;

24.2.4 the methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed by the Data Protection Officer;

24.2.5 all agents, contractors, or other parties handling personal data on behalf of VIRIDIAN shall ensure that any and all relevant employees are held to the same conditions as those relevant employees of VIRIDIAN arising out of the Data Protection Laws and the this Policy;

24.2.6 where any agent, contractor or other party handling personal data on behalf of VIRIDIAN fails in their obligations under the Data Protection Laws and/or this Policy, that party shall indemnify and hold harmless VIRIDIAN against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

## **25. RELATED ENTITIES**

VIRIDIAN is a for-profit company, which is a related party to African Entrepreneurship Ecosystem Investors (AEEI), a non-profit company registered in the Republic of South Africa under registration number 2021/593658/08. VIRIDIAN and AEEI work closely on a number of matters, and accordingly, personal data collected by one of the entities is sometimes shared amongst and processed by both of the entities. This is only done in accordance with this Policy and the applicable Data Protection Laws.

## **26. TRANSFERRING PERSONAL DATA TO ACROSS BORDERS**

26.1 VIRIDIAN may, from time to time, transfer personal data to countries outside of the country in which the personal data was collected, but only where one of the following principles applies:

26.1.1 where the country in question is subject to laws, or policies, which uphold principles for the reasonable processing of information substantially similar to the Data Protection Laws applicable to the jurisdiction in which the personal data was collected;

- 26.1.2 where there are appropriate safeguards are in place, including binding corporate rules, and/or standard contractual clauses approved for use in terms of Data Protection Laws, an approved code of conduct, or an approved certification mechanism.
- 26.1.3 the transfer is made with the informed and explicit consent of the relevant data subject(s); or
- 26.1.4 the transfer is necessary for one of the other reasons set out in Data Protection Laws, including the performance of a contract between the data subject and VIRIDIAN; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for VIRIDIAN's legitimate interests.

## **27. DATA BREACH NOTIFICATION**

- 27.1 All personal data breaches must be reported immediately to VIRIDIAN's Data Protection Officer.
- 27.2 If an employee, agent, contractor, or other party working on behalf of VIRIDIAN becomes aware of or suspects that a personal data breach has occurred, they shall not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.
- 27.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer shall ensure that the relevant regulator's office is informed of the breach without delay (within 72 hours, where GDPR is applicable).
- 27.4 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer shall ensure that all affected data subjects are informed of the breach directly and without undue delay.
- 27.5 Data breach notifications shall include the following information:
  - 27.5.1 the categories and approximate number of data subjects concerned;
  - 27.5.2 the categories and approximate number of personal data records concerned;
  - 27.5.3 the name and contact details of the Data Protection Officer;
  - 27.5.4 the likely consequences of the breach; and
  - 27.5.6 details of the measures taken, or proposed to be taken, by VIRIDIAN to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Name:	Alexandra Fraser
Position:	Director
Date:	21 October 2021
Signature:	