DIGITAL FRONTIERS NPC

DATA PROTECTION POLICY

Approved by:	Gavin Krugel	**Issued:**	July 2022

*By accessing, viewing, or engaging with this Data Protection Policy, you acknowledge and consent to the collection, processing, and use of your data as outlined herein. You agree that your continued use of Digital Frontiers' platforms and services constitutes acceptance of this policy. Digital Frontiers assumes no legal liability for any claims, losses, or damages arising from your consent to this policy or your engagement with its terms. Your use of our services signifies your acceptance of these conditions.

CONTENTS

1. INTRODUCTION AND PURPOSE

1.1. This policy ("**Policy**") sets out the data protection principles and procedures of Digital Frontiers, a non-profit company registered in the Republic of South Africa under registration number 2017/127296/08, whose registered office is at Office No.3, Watershed, 17 Dock Road, V&A Waterfront, Cape Town, 8002 (the "**Organisation**").

1.2. In particular, this Policy summarises how the Organisation processes **personal information** belonging to, amongst others, its staff, business contacts, clients, and suppliers ("**data subjects**").

1.3. The Organisation takes the privacy of **personal information** very seriously, and is committed to **processing personal information** in accordance with data protection legislation, including the Protection of Personal Information Act (No. 4 of 2013) ("**POPI**") and, where applicable, the General Data Protection Regulation (EU 2016/679) ("**GDPR**"), which includes the retained EU law version of GDPR as it forms part of the law of the United Kingdom, and any other data protection legislation and/ or regulation applicable to the Organisation (collectively, the "**Data Protection Laws**").

1.4. This Policy is made available on the Organisation's websites (https://digitalfrontiersinstitute.org/, https://digitalfrontiers.org/, https://alliancedfa.org/ and https://twentyforgood.org/

1.5. The Organisation's **Information Officer's** details are:

Information Officer:	Xavier Palomas
Telephone:	+ 27 (0) 21 201 7299
E-mail:	xavier@digitalfrontiers.org

1.6. This Policy uses terminology defined in POPI (these terms appear in bold). Please see paragraph 24 of this Policy for the definitions applicable to this terminology and for guidance in interpreting this Policy.

1.7. **Please note: The Organisation's website ("Website") may contain links to third-party websites. The Organisation is not responsible for the privacy practices or the content of third-party sites. The relevant user or data subject must carefully read the privacy policy of any website visited.**

2. SCOPE

The procedures and principles set out in this Policy must be followed at all times by the Organisation's employees, agents, contractors, affiliates, and other parties working on behalf of the Organisation, including third-party **operators processing personal information** on the Organisation's behalf ("**third-party operators**"), which third-party operators must also be compliant with Data Protection Laws. No **personal information** must be **processed** for or on the Organisation's behalf unless **processed** in accordance with this Policy and Data Protection Laws.

3. INFORMATION OFFICER

3.1. The **Information Officer** is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/ or guidelines in accordance with Data Protection Laws.

3.2. The **Information Officer** is tasked with ensuring that all employees, agents, contractors, affiliates, and other parties working on behalf of the Organisation, including third-party operators, comply with this Policy. The **Information Officer** is also responsible for monitoring and ensuring compliance with the GDPR and other applicable Data Protection Laws, managing internal data protection activities, advising on data protection impact assessments, training staff, and conducting internal audits.

3.3. Any questions relating to this Policy or to Data Protection Laws should be referred to the Organisation's **Information Officer –** please see contact details provided below as well as clause 24 (*Queries*).

3.4. The **Organisation**'s employees, agents, contractors, affiliates, and other parties working on behalf of the **Organisation**, including third-party operators behalf must consult the **Information Officer** in the following cases:

3.4.1. If there is any uncertainty relating to the lawful basis on which **personal information** is to be collected, held, and/ or **processed**;

3.4.2. If **consent** is being relied upon in order to collect, hold, and/ or **process personal information**;

3.4.3. If there is any uncertainty relating to the retention period for any particular type(s) of **personal information**;

3.4.4. 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);

3.4.5. If a **personal information breach** (whether suspected or actual) has occurred;

3.4.6. If there is any uncertainty relating to security measures (whether technical or organisational) required to protect **personal information**;

3.4.7. If **personal information** is to be shared with third parties (whether such third parties are acting jointly as **responsible parties** or operators);

3.4.8. If **personal information** 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;

3.4.9. When any significant new **processing** activity is to be carried out, or significant changes are to be made to existing **processing** activities;

3.4.10. When **personal information** is to be used for purposes different to those for which it was originally collected;

3.4.11. If any automated **processing**, including profiling or automated decision-making, is to be carried out; or

3.4.12. If any assistance is required in complying with the law applicable to direct marketing.

4. THE RIGHTS OF DATA SUBJECTS

4.1. Data subjects have the right to have their **personal information processed** in accordance with the conditions for the lawful **processing** of **personal information** as referred to in the Data Protection Laws. The Organisation is committed to upholding the rights of data subjects, which rights include:

4.1.1. The right to be notified/informed (Articles 12, 13, and 14 GDPR): data subjects must be informed when their **personal information** is collected or changed;

4.1.2. The right of access (Article 15 GDPR): data subjects may request confirmation and access to their **personal information**;

4.1.3. The right to rectification (Article 16 GDPR): data subjects may request corrections to inaccurate **personal information**;

4.1.4. The right to correction, destruction or erasure (the "right to be forgotten") (Article 17 GDPR): data subjects may request correction, destruction, or erasure of their **personal information** under certain conditions;

4.1.5. The right to object to or restrict processing (Articles 18 and 21 GDPR): data subjects may object or request restrictions on the **processing** of their **personal information**;

4.1.6. The right to data portability (Article 20 GDPR): data subjects may receive their **personal information** in a usable format and transfer it to another entity;

4.1.7. Rights with respect to automated decision-making and profiling (Article 22 GDPR): data subjects may avoid decisions made solely on automated **processing**;

4.1.8. The right to complain to the Regulator / supervisory authority (Article 77 GDPR): data subjects may lodge complaints with the relevant data protection authority – see clause 24 (*Queries*);

4.1.9. The right to institute civil proceedings in relation to its **personal information**: data subjects may take legal action if their data rights are violated;

4.1.10. The right to judicial review (Articles 79 and 82 GDPR): data subjects may seek judicial review of data protection decisions; and

4.1.11. The right to withdraw **consent** (Article 7 GDPR): data subjects may withdraw their **consent** for data **processing** at any time.

4.2. Data subjects may exercise any of the above rights by:

4.2.1. contacting (or directing any data-related queries to) the **Information Officer** using the contact details provided in this Policy, who will deal with the matter promptly; or

4.2.2. following the relevant prompts contained in the relevant e-mail communications received.

5. DATA PROTECTION PRINCIPLES

5.1. The Organisation is committed to promoting and upholding the conditions for the lawful **processing** of **personal information** as set out in the Data Protection Laws, being:

5.1.1. Accountability, as contemplated in section 8;

5.1.2. **Processing** limitation and data minimisation, as contemplated in sections 9 – 12: limited to what is necessary in relation to the purpose for which it is **processed**;

5.1.3. Purpose specification, as contemplated in sections 13 – 14;

5.1.4. Further **processing** limitation, as contemplated in section 15;

5.1.5. Information quality, as contemplated in section 16;

5.1.6. Openness and transparency, as contemplated in sections 17 – 18;

5.1.7. Security safeguards, as contemplated in sections 19 – 22;

5.1.8. Data subject participation, as contemplated in sections 23 – 25;

5.1.9. Fairness;

5.1.10. Accuracy;

5.1.11. Storage limitation;

5.1.12. Integrity; and

5.1.13. Confidentiality.

5.2. Accordingly, the Organisation is committed to **processing personal information** only in a manner that:

5.2.1. Is lawful and transparent;

5.2.2. Is specified, explicit, and legitimate, and for a particular purpose;

5.2.3. Is relevant, and limited to what is necessary in relation to the purposes for which it is **processed**;

5.2.4. Is accurate;

5.2.5. Permits identification of data subjects for no longer than is necessary for the lawful purposes for which the **personal information** was collected and/or **processed** or insofar as permitted by Data Protection Laws; and

5.2.6. Ensures appropriate security of the **personal information**, including protection against unauthorised or unlawful **processing** and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

6. PROCESSING OF PERSONAL INFORMATION

6.1. **Data subjects are responsible for ensuring that the personal information they provide to the Organisation is accurate, complete, and up to date. Data subjects must promptly inform the Organisation of any changes to their personal information to maintain its accuracy and completeness.**

6.2. The Organisation shall only **process personal information** if at least one of the following lawful bases apply (Article 6 GDPR):

6.2.1. The data subject (or a **competent** person, where the data subject is a **child**) has provided **consent** to the **processing**. When the data subject submits information to the Organisation, the data subject **consent** to the Organisation **processing** that **personal information**, but may withdraw this **consent** at any time;

6.2.2. **Processing** is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering a contract;

6.2.3. **Processing** is necessary for compliance with an obligation imposed by law on the **responsible party**;

6.2.4. **Processing** is necessary to protect a legitimate or vital interest of the data subject (except where overridden by the interests or fundamental rights and freedoms of the data subject which require protection of **personal information**, particularly where the data subject is a **child**) or another natural person;

6.2.5. **Processing** is necessary for the proper performance of a public law duty by a public body; and/ or

6.2.6. **Processing** is necessary for pursuing the legitimate interests of the **responsible party** or of a third party to whom the information is supplied.

6.1. Subject to the above, the Organisation may collect and **process** information submitted by a data subject, such as name and contact details, or non-personally identifiable information (i.e., anonymous data), to provide the services, personalise the data subject's Website experience, develop new services, analyse the services, review Website usage, contact the data subject, for marketing (with an opt-out option), provide course information, respond to queries, for other legitimate business purposes, and to verify identity.

6.2. Where a person transmits any **personal information** to the Organisation which belongs to a third party, that person warrants that they are duly authorised to do so and that the **processing** of the **personal information** by the Organisation is lawful. Each such person hereby indemnifies the Organisation to the fullest extent permitted by law for any loss as a result of disclosing **personal information** without the requisite authority. **If a data subject knows or suspects that unauthorised disclosure or use of personal information has occurred, such data subject must contact the Information Officer immediately.**

6.3. Subject to the above, the Organisation may share **personal information** and non-personally identifiable or anonymised data:

6.3.1. With donors and/or funders to generate reports on pass/fail rates and for statistical reasons, to analyse participation (the information provided will not be personally identifiable);

6.3.2. With service providers, affiliates, and related entities to render the services, and/or for internal administration purposes;

6.3.3. To comply with any law, regulation, legal process, or governmental request;

6.3.4. To protect the security of the Website, the Organisation's servers, network systems, and databases and/or

6.3.5. To combat fraud.

6.4. The Organisation implements a variety of security measures to maintain the safety of data subject/s **personal information** in accordance with Data Protection Laws, including those measures set out in this clause 6. However, please note that no data transmission over the internet can be guaranteed to be 100% secure. If there is a **personal information** breach, the Organisation will take all necessary steps to mitigate its impact, inform the affected data subjects, and notify relevant authorities, as required by Data Protection Laws. While the Organisation strives to protect data subjects' personal information, **the Organisation cannot be held liable for breaches caused by factors beyond its reasonable control, provided that the Organisation has complied with its obligations under Data Protection Laws**.

7. PROCESSING OF SPECIAL PERSONAL INFORMATION

The Organisation shall only **process special personal information** in accordance with Data Protection Laws. The **processing** of **special personal information** shall be lawful if at least one of the following applies:

7.1. **Processing** is carried out with the **consent** of a data subject;

7.2. **Processing** is necessary for the establishment, exercise or defence of a right or obligation in law;

7.3. **Processing** is necessary to comply with an obligation of international public law;

7.4. **Processing** is for historical, statistical or research purposes to the extent that:

7.4.1. The purpose serves a public interest and the **processing** is necessary for the purpose concerned; or

7.4.2. It appears to be impossible or would involve a disproportionate effort to ask for **consent**, and sufficient guarantees are provided for to ensure that the **processing** does not adversely affect the individual privacy of the data subject to a disproportionate extent;

7.5. Information has deliberately been made public by the data subject; or

7.6. Where applicable, the provisions of sections 28 to 33 of POPI, as the case may be, are complied with.

8. PROCESSING OF PERSONAL INFORMATION RELATING TO CHILDREN

8.1. The Organisation shall only **process personal information** relating to a **child** in accordance with Data Protection Laws. The **processing** of **personal information** relating to a **child** shall be lawful if at least one of the following applies:

8.1.1. The **processing** is carried out with the prior **consent** of a **competent** person (such as a parent or legal guardian);

8.1.2. The **processing** is necessary for the establishment, exercise or defence of a right or obligation in law, or to comply with the law or a court order;

8.1.3. The **processing** is necessary to protect the vital interests of the **child** or another natural person where the **child** is incapable of giving **consent**;

8.1.4. The **processing** is carried out in the course of the legitimate activities of a foundation, association, or any other not-for-profit body with a political, philosophical, religious, or trade union aim, provided that the **processing** relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and that the **personal information** is not disclosed outside that body without the requisite **consent** of the **competent** person;

8.1.5. The **processing** is necessary for reasons of substantial public interest (where applicable, on the basis of the Union or Member State 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**; and/or

8.1.6. The relevant **personal information** has deliberately been made public by the **child** with the **consent** of a **competent** person.

8.2. The Organisation does not market to, nor does it provide the services to **children**. Accordingly, the Organisation does not knowingly **process** any **personal information** belonging to **children**. If the Organisation learns that a **child's personal information** has been unlawfully submitted to us, the Organisation will take reasonable steps to delete the **child's personal information** promptly and inform the **child's** parent or guardian of the situation.

9. ACCURACY OF PERSONAL INFORMATION

9.1. The Organisation shall ensure that all **personal information** collected, **processed**, and held by it is kept accurate and up to date in accordance with Data Protection Laws.

9.2. If any **personal information** is found to be inaccurate or out-of-date, the **Information Officer** must be notified immediately.

10. STORAGE AND RETENTION

10.1. Personal information, is stored by the Organisation in the following ways and in the following locations:

10.1.1. Third-party servers, operated by, amongst others:

10.1.1.1. Absolute Cloud Solutions (ACS), and located in Cape Town, South Africa;

10.1.1.2. OpenCollab (Pty) Ltd, and located in Cape Town, South Africa;

10.1.1.3. Tableau, and located in Seattle, USA;

10.1.2. Computers permanently located at the Organisation's business premises;

10.1.3. Laptop computers and other mobile devices provided by the Organisation to its employees, agents, and contractors;

10.1.4. Computers and mobile devices owned by employees, agents, and contractors; and

10.1.5. Physical records stored at the Organisation's premises, or the premises of the Organisation's partners/ affiliates.

10.2. When **personal information** is no longer required for the intended purpose it was collected and/or **processed** (i.e., when the retention period expires), it will either be **de-identified**, or all reasonable steps will be taken to erase or otherwise dispose of it without delay.

10.3. **Personal information** may be stored for longer periods insofar as the **personal information** will be **processed** solely for archiving purposes in the public interest, scientific or historical research, or statistical purposes subject to implementation of the appropriate technical and organisational measures required by Data Protection Laws in order to safeguard the rights and freedoms of the data subject/s.

10.4. A **data subject** may request that the Organisation erase any **personal information** it holds about them. Upon receiving such a request, the Organisation will erase the **data subject's personal information** without undue delay, cease further dissemination of the **personal information**, and notify any third parties processing the **data subject's personal information** to halt further **processing** and erase / de-identify such **personal information** in accordance with Data Protection Laws.

11. SECURE PROCESSING

11.1. The Organisation shall ensure that all **personal information** collected, held, and **processed** by it is kept secure and protected against unauthorised or unlawful **processing** and against accidental loss, destruction, or damage in accordance with Data Protection Laws.

11.2. All technical and organisational measures taken to protect **personal information** shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of **personal information**.

11.3. The Organisation will adhere to the following guidelines to protect against the confidentiality, integrity, and availability of all **personal information**:

11.3.1. Only those with a genuine need to access and use **personal information** and who are authorised to do so may access and use it;

11.3.2. **Personal information** must be accurate and suitable for the purpose for which it is collected, held, and **processed**; and

11.3.3. Authorised users must always be able to access the **personal information** as required for the authorised purpose or purposes.

12. COOKIES & THIRD-PARTY TECHNOLOGIES

12.1. "**Cookies**" are small files stored on the data subject's computer during use of the Website and which contain data about the data subject's use of the Website. The Organisation may use session Cookies (which expire when a browser is closed) or persistent Cookies (which stay on a computer until deleted) for various purposes, including:

12.1.1. Authenticating users;

12.1.2. Remembering preferences and settings;

12.1.3. Determining the popularity of Website content;

12.1.4. Delivering and measuring the effectiveness of advertising campaigns;

12.1.5. Analysing site traffic and trends; and

12.1.6. Enhancing security.

12.2. A data subject can control the technologies the Organisation uses by using the settings in their browser or third-party tools.

13. ACCOUNTABILITY AND RECORD-KEEPING

13.1. A data protection impact assessment (DPIA) shall be conducted by the Organisation prior to **processing** of **personal information** if it presents a high risk to the rights and freedoms of data subjects, in accordance with the GDPR (Article 35).

13.2. The Organisation's data protection compliance will be regularly and continuously reviewed and evaluated by the **Information Officer**.

13.3. The Organisation will keep adequate internal records of **processing** activities in respect of the **processing** of **personal information** in accordance with Data Protection Laws.

14. RECTIFICATION OF PERSONAL INFORMATION

14.1. Data subjects have the right to require the Organisation to rectify any of their **personal information** that is inaccurate or incomplete, in accordance with Data Protection Laws. The Organisation shall comply with such requests timeously.

14.2. In the event that any affected **personal information** has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that **personal information**.

15. ERASURE OF PERSONAL INFORMATION

15.1. Data subjects have the right to request that the Organisation erases the **personal information** it holds about them in certain circumstances, for example, where the data subject withdraws their **consent** for the **processing** of their **personal information** in accordance with Data Protection Laws.

15.2. Unless the Organisation has reasonable grounds to refuse to erase **personal information**, all requests for erasure shall be complied with timeously, and the data subject informed of the erasure.

15.3. If any **personal information** 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).

16. RESTRICTION OF PERSONAL INFORMATION PROCESSING

16.1. A data subject may at any time request that the Organisation ceases **processing** the **personal information** it holds about them, in accordance with Data Protection Laws. If a data subject makes such a request, the Organisation shall retain only the amount of **personal information** concerning that data subject (if any) that is necessary to ensure that the **personal information** in question is not **processed** further, or unless otherwise required by law.

16.2. If any affected **personal information** 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). The Organisation will inform the data subject about such third parties if the data subject requests it.

17. DATA PORTABILITY

Data subjects have the right to receive a copy of their **personal information** in the Organisation's possession in a structured, commonly used and machine-readable format, and to request its transmission to another entity, in accordance with Data Protection Laws.

18. OBJECTIONS TO PROCESSING PERSONAL INFORMATION

18.1. Data subjects have the right to object to the Organisation **processing** their **personal information** based on legitimate interests, for direct marketing (including profiling), and **processing** for research and statistics purposes, in accordance with Data Protection Laws.

18.2. Where a data subject objects to the Organisation **processing** their **personal information** based on its legitimate interests, the Organisation shall cease such **processing** immediately, unless the Organisation demonstrates that its 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.

18.3. Where a data subject objects to the Organisation **processing** their **personal information** for direct marketing purposes, the Organisation shall cease such **processing** promptly.

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

19. DIRECT MARKETING

19.1. The Organisation shall obtain a data subject's prior **consent** for direct marketing (including email and text messaging), in accordance with Data Protection Laws. This **consent** shall be specific, distinguishable from other matters, and provided in an intelligible and easily accessible form. Additionally, the Organisation shall ensure that withdrawing **consent** is as easy as giving it.

19.2. The Organisation shall not approach a data subject more than once for the purpose of obtaining their **consent** to direct marketing.

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

19.4. The Organisation will not approach a data subject for purposes of direct marketing if that data subject has previously withheld **consent**.

20. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

20.1. Mandated measures. The following technical and organisational measures shall be implemented to protect the security of **personal information**, in accordance with Data Protection Laws:

20.1.1. Appropriate firewalls and anti-virus protections should be implemented, and regular malware scans shall be conducted;

20.1.2. **Personal information** should only be transmitted over secure networks;

20.1.3. All **personal information** transferred physically should be transferred in a suitable container and marked "confidential";

20.1.4. All hardcopies of **personal information**, along with any electronic copies stored on physical media should be stored securely and appropriate access control measures should be implemented;

20.1.5. All electronic copies of **personal information** will be stored securely using passwords and where appropriate, be encrypted; and

20.1.6. The methods of collecting, holding, and **processing personal information** will be regularly evaluated and reviewed by the **Information Officer**.

20.2. Recommended best practices. Where possible, the Organisation will use best endeavours to implement the following technical and organisational measures to implement to protect the security of personal information, as recommended best practices:

20.2.1. No **personal information** may be shared informally, and if access is required in respect of any **personal information**, such access should be requested in writing;

20.2.2. **Personal information** must be handled with care at all times and should not be left unattended;

20.2.3. All passwords used to protect **personal information** will be changed regularly;

20.2.4. No passwords will be written down or shared with others. If a password is forgotten, it must be reset using the applicable method; and

20.2.5. No unauthorised software may be installed on any computer or device owned by the Organisation, without prior written approval from the **Information Officer**.

20.2.6. All employees and other parties working on behalf of the Organisation will be bound to comply with the Data Protection Laws and this Policy;

20.2.7. All employees and other parties handling **personal information** on behalf of the Organisation will exercise care and caution when discussing any work relating to **personal information**; and

20.2.8. All agents, contractors, or other parties handling **personal information** on behalf of the Organisation will ensure that all persons who have access to such **personal information** are held to the same degree of care as contemplated in this Policy.

20.3. Suggested additional measures. Where possible, the following technical and organisational measures may be implemented to protect the security of personal information, as recommended best practices:

20.3.1. Regular training and awareness programs will be conducted for all employees and contractors on data protection and security best practices;

20.3.2. Incident response plans will be established, including steps to be taken in the event of a personal information breach;

20.3.3. DPIAs will be conducted for any processing activities that pose a high risk to the rights and freedoms of data subjects;

20.3.4. Role-based access control (RBAC) and regular monitoring of access logs will be implemented to ensure that only authorised personnel have access to personal information;

20.3.5. Data minimisation and anonymisation practices will be adopted wherever possible to reduce privacy risks;

20.3.6. Regular security audits and vulnerability assessments will be conducted to ensure the effectiveness of security measures;

20.3.7. Industry-standard encryption protocols will be used for personal information at rest and in transit;

20.3.8. Data backup and disaster recovery plans will be established to ensure quick recovery in the event of personal information loss incidents;

20.3.9. Regular assessments and audits of third-party compliance will be conducted to manage third-party risks; and

20.3.10. Clear data retention policies will be established, including timelines for different types of personal information and secure disposal processes.

20.4. Where any agent, contractor or other party processes **personal information** on behalf of the Organisation fails in their obligations under the Data Protection Laws and/or this Policy, that party, by way of entering the relevant agreement with the Organisation, indemnifies and holds harmless the Organisation, to the furthest extent permitted in law, against any and all costs, liability, damages, loss, claims or proceedings, of whatever nature and howsoever arising out of or attributable in any way to such act/s or omission/s.

21. TRANSFERRING PERSONAL INFORMATION ACROSS BORDERS (NOT APPLICABLE TO EU/EEA OR UK REGION)

The Organisation may, from time to time, transfer **personal information** to countries outside of the country in which the **personal information** was collected, but only where one of the following principles applies:

21.1. The third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that:

21.1.1. Effectively upholds the principles for **processing** personal information as set out in the Data Protection Laws for the lawful **processing** of **personal information** relating to a data subject who is a natural person and, where applicable, a juristic person; and

21.1.2. Includes provisions, that are substantially similar to this section, relating to the further transfer of **personal information** from the recipient to third parties who are in a foreign country;

21.2. The data subject **consents** to the transfer;

21.3. The transfer is necessary for the performance of a contract between the data subject and the **responsible party**, or for the implementation of pre-contractual measures taken in response to the data subject's request;

21.4. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the **responsible party** and a third party; or

21.5. The transfer is for the benefit of the data subject, and:

21.5.1. It is not reasonably practicable to obtain the **consent** of the data subject to that transfer; or

21.5.2. If it were reasonably practicable to obtain such **consent**, the data subject would have the option to give it.

22. TRANSFERRING PERSONAL INFORMATION ACROSS BORDERS (APPLICABLE TO EU/EEA OR UK REGION)

The Organisation may, from time to time, transfer **personal information** to countries outside of the country in which the **personal information** was collected (whether this be the EU/EEA region or the UK region), but only where one of the following principles applies, in accordance with Chapter V of the GDPR:

22.1. The third party who is the recipient of the **personal information** is located in a country that the European Commission has decided provides an adequate level of protection for personal information (Article 45).

22.2. The transfer is subject to appropriate safeguards, such as:

22.2.1. The third party is subject to binding corporate rules approved by the relevant supervisory authority (Article 47);

22.2.2. The transfer is based on standard data protection clauses adopted by the European Commission or such other relevant authority (Article 46(2)); and

22.2.3. Other legally binding instruments that provide appropriate safeguards (Article 46).

22.3. The data subject has explicitly **consented** to the proposed transfer, after being informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards (Article 49(1)(a)).

22.4. The transfer is necessary for the performance of a contract between the data subject and the **responsible party**, or for the implementation of pre-contractual measures taken at the data subject's request (Article 49(1)(b)).

22.5. The transfer is necessary for important reasons of public interest (Article 49(1)(d)).

22.6. The transfer is necessary for the establishment, exercise, or defence of legal claims (Article 49(1)(e)).

22.7. The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving **consent** (Article 49(1)(f)).

22.8. The transfer is made from a register which, according to Union or Member State law, is intended to provide information to the public and which is open to consultation by the public in general or by any person who can demonstrate a legitimate interest (Article 49(1)(g)).

22.9. The transfer is for the benefit of the data subject, and:

22.9.1. it is not reasonably practicable to obtain the **consent** of the data subject for that transfer; or

22.9.2. if it were reasonably practicable to obtain such **consent**, the data subject would have the option to give it (Article 49(1)(c)).

23. PERSONAL INFORMATION BREACH NOTIFICATION

23.1. If an employee, agent, contractor, or other party working on behalf of the Organisation becomes aware of or suspects that a **personal information breach** has occurred, they will notify an **Information Officer** immediately, and will not attempt to investigate it themselves. All evidence relating to the **personal information breach** in question should be carefully retained.

23.2. Where there are reasonable grounds to believe that the **personal information** of a data subject has been accessed or acquired by any unauthorised person, the Organisation will, as soon as reasonably possible, notify, in writing:

23.2.1. The **Regulator** (such notification to be within 72 hours, where GDPR is applicable); and

23.2.2. The data subject without undue delay, unless:

23.2.2.1. the identity of such data subject cannot be established (i.e., the personal information has been anonymised or encrypted); or

23.2.2.2. the Organisation has taken subsequent measures to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to occur; or

23.2.2.3. it would involve a disproportionate amount of effort, in which case the Organisation will issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

23.3. The notification referred to in clause 23.2 above will include, at a minimum, the following information:

23.3.1. A description of the nature of the **personal information** breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of **personal information** records concerned;

23.3.2. The name and contact details of the **Information Officer** or other contact point where more information can be obtained;

23.3.3. A description of the likely consequences of the **personal information** breach; and

23.3.4. A description of the measures taken or proposed to be taken by the **responsible party** to address the **personal information** breach, including, where appropriate, measures to mitigate its possible adverse effects.

23.4. The Organisation may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the **Regulator** determines that notification will impede a criminal investigation by the public body concerned.

24. QUERIES

24.1. If data subject would like to exercise any of their rights in respect of their personal information or has any queries or complaints on how the Organisation handles personal information, the data subject must contact the **Information Officer**.

24.2. Data subjects also have the right to lodge a complaint with the relevant regulatory body, which for the purposes of POPI in South Africa, is the Information Regulator. The Information Regulator can be contacted by email at complaints.IR@justice.gov.za or inforeg@justice.gov.za.

25. AMENDMENTS

The Organisation reserves the right to amend this Policy at any time. In case of any material changes affecting the processing of personal information, the Organisation will notify the data subjects in a clear and timely manner.

26. DEFINITIONS

26.1. In this Policy, the following words mean (whether used in capitalised or lowercase form):

26.1.1. **Child**. A natural person under the age of 18 years who is not legally **competent**, without the assistance of a **competent** person, to take any action or decision in respect of any matter concerning him- or herself.

26.1.2. **Competent person**. Any person who is legally **competent** to **consent** to any action or decision being taken in respect of any matter concerning a **child**.

26.1.3. **Consent**. Any voluntary, unambiguous, specific and informed expression of will in terms of which permission is given for the **processing** of **personal information**.

26.1.4. **De-identify**. In relation to **personal information** of a data subject, to pseudonymise or delete any information that:

26.1.4.1. Identifies the data subject;

26.1.4.2. Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

26.1.4.3. Can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and ''**de-identified**'' has a corresponding meaning.

26.1.5. **Information Officer**. "*Information Officer*" as contemplated in POPI and/or "*Data Protection Officer*" as contemplated in the GDPR, as applicable.

26.1.6. **Operator**. A person who processes **personal information** for a **responsible party** in terms of a contract or mandate, without coming under the direct authority of that party.

26.1.7. **Personal information**. 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, including "*personal data*" as defined in the GDPR.

26.1.8. **Personal information breach**. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to **personal information** transmitted, stored, or otherwise **processed**.

26.1.9. **Process**. Any operation or set of operations performed on **personal information** or sets of **personal information**, 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.

26.1.10. **Regulator**. The Information Regulator established in terms of section 39 of POPI, and/or the relevant "*supervisory authority*" as contemplated in the GDPR.

26.1.11. **Responsible party**. A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for **processing personal information**, including "*data controller*" as defined in the GDPR .

26.1.12. **Special personal information**. As contemplated in section 26 of POPI, which includes religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, genetic or biometric information of a data subject; and/or the criminal behaviour of a data subject to the extent that such information relates to:

26.1.12.1. The alleged commission by a data subject of any offence; or

26.1.12.2. Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings,

and includes "*special categories of personal data*" as contemplated in the GDPR.

26.2. In this Policy:

26.2.1. The words "**include**", "**including**" and "**in particular**" are by way of example only and shall not limit the generality of any preceding words;

26.2.2. 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 Policy; and

26.2.3. The words "**other**" and "**otherwise**" shall be interpreted as widely as possible and will not be limited by any preceding words.

26.3. This Policy has been drafted using the terminology contemplated in POPI. Where this Policy is interpreted in the context of GDPR, the terms:

26.3.1. "I**nformation Officer**" shall be read as "**Data Protection Officer**";

26.3.2. "**Responsible party**" shall be read as " **data controller**";

26.3.3. "**Personal information**" shall be read as " **personal data**";

26.3.4. "**Regulator**" shall be read as "**Supervisory Authority**"; and

26.3.5. "**Special personal information**" shall be read as "**special category personal information**",

as those terms are defined in GDPR.

The Organisation reserves the right to amend this Policy at any time. In case of any material changes affecting the processing of personal information, the Organisation will notify the data subjects in a clear and timely manner.