DATA PROTECTION POLICY OF A2D24

Revision date: 04 August 2020

Approval date: 07 August 2020

Approved by: Sofiah Docrat

DATA PROTECTION POLICY OF A2D24

TABLE OF CONTENTS

1. Forward 3
2. Key descriptions 4
3. Appointment of information officers 6
4. Conditions for lawful processing 7
5. Special Personal Information 9
6. Retention of Records 10
7. Security safeguards 10
8. Use of operators to process information 11
9. Information Security 12
10. Notification of a Personal Information Security Breach 13
11. client's access to information 14
12. Separation of Personal Information 15
13. Access to information 16
14. Correction of personal information 16

1. Forward

1.1 A2D24 is the custodian of our client's personal data / information including financial data as well as stakeholders' and the organisations' data/ information and we are committed to protecting this information by ensuring compliance with all applicable legislation and regulations as well as internationally recognised standards within the jurisdictions that we operate in.

1.2 This includes those laws and regulations and standards relative to:

1.2.1 Personal information (this includes information held for clients, stakeholders, and employees);

1.2.2 Information Technology, and

1.2.3 Information Security.

1.3 We view data privacy and Information Security as fundamental components of doing business. As such, we are committed to protecting personal data and client information wherever they are created, processed, transmitted or stored.

1.4 This Data Protection Policy was developed to provide clear guidance to all our employees and to ensure a consistent approach to business practices throughout our operations.

1.5 We are also committed to maintaining the highest ethical standards and to complying with all laws and regulations applicable to the conduct of our business, including those relating to protection of data. A2D24 recognises that everyone has the right to privacy, and that the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of data which constitutes Personal Information.

1.6 The objective of this Data Protection Policy ("Policy") is to –

1.6.1 set out the practices and responsibilities A2D24 and each employee in A2D24 undertakes in order to protect the privacy of clients, business partners, third party stakeholders, employees and of A2D24;

1.6.2 establish rules and procedures to protect confidential information and avoid security threats by promoting awareness and good practice;

1.6.3 clarify the practises and procedures that enable A2D24 to monitor and audit compliance with the Policy and to set out consequences of non-compliance; and

1.6.4 minimise the inherent risks of non-compliance to local and international privacy legislation, including but not limited to reputational damage, regulatory sanctions and loss of A2D24's intellectual property;

1.6.5 The Policy is not intended to reproduce laws or regulations but rather to set out guidelines for behaviour for A2D24 and its employees and provide guidance to A2D24, which are responsible for developing and implementing the requirements of the Policy and effectuating compliance with the laws and regulations to which we may be subject.

1.6.6 It is the responsibility of every employee to behave according to the principles laid out in this Policy.

2. Key descriptions

2.1 "**Data Holder**" means the person appointed to hold and deal with personal data as instructed by the Data Owner for the specific purpose of providing data processing and/or storage services, as contemplated in this Policy;

2.2 "**Data Subjects**" means either Parties' Affiliates, clients, employees, ex-employees and any other person/s to whom Personal Information relates;

2.3 "**Data Owner**" means the person who has the authority to decide on the access to, and usage of, any personal data, as contemplated in this Policy;

2.4 "**Information Technology**" means the use of systems (especially computers and telecommunications) for storing, retrieving, and sending information

2.5 "**Information Security**", means the practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

2.6 "**POPI Act**" means the Protection of Personal Information Act No. 4 of 2013;

2.7 "**Processing**" or "**Process**" has the meaning set out in POPI Act

2.8 "**Data Subject**' means the natural person or juristic person to whom Personal Information relates.

2.9 "**Personal Information**" has the meaning set out in the POPI Act, and relates only to the Personal Information of which client is the Responsible Party and includes information relating to an identifiable, living, natural person, and where it is applicable; an identifiable, existing juristic person, including, but not limited to-

2.9.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

2.9.2 information relating to the education or the medical, financial, criminal or employment history of the person;

2.9.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

2.9.4 the biometric information of the person;

2.9.5 the personal opinions, views or preferences of the person;

2.9.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

2.9.7 the views or opinions of another individual about the person; and

2.9.8 the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.9.9 "**Process/Processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including-

2.9.9.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.9.9.2 dissemination by means of transmission, distribution or making available in any other form; or

2.9.9.3 merging, linking, as well as restriction, degradation, erasure or destruction of information;

2.10 "**Regulator**" means the appropriate Regulator as defined in applicable Personal Information protection legislation;

2.11 "**Responsible Party**" means the person who, alone or in conjunction with others, determines the purpose of and means for Processing Personal Information, and who is also the client of A2D24;

2.12 "**A2D24**", "**A2D24 Group**" or "**we**" refers to one or more of A2D24 Dot Com (Pty) Ltd, any of our holding company, subsidiaries, sister company, employees, officers, advisors and affiliates (hereinafter "A2D24" or "A2D24 Entity").

3. Appointment of information officers

3.1 Each A2D24 Entity is expected to comply with the Policy and to hire and train personnel in accordance with the Policy, including designating or appointing an Information Officer and Deputy Information Officers (if required). Each A2D24 Entity is responsible in the first instance for complying with laws and regulations applicable to that A2D24 Entity. Information Officers shall be responsible for –

3.1.1 ensuring and encouraging compliance with this Policy and applicable laws in order to ensure the lawful Processing of Personal Information by each A2D24 Entity;

3.1.2 dealing with requests made to an A2D24 Entity for access to Personal Information held by that A2D24 Entity;

3.1.3 liaising with Regulators; and

3.1.4 providing training to employees.

3.1.5 Employees must report any questions, concerns, possible violations, and reportable conditions to the designated Information Officer. The Information Officer(s) shall be responsible for administration of this Policy and shall ensure that any relevant authorities are notified of any violations or reportable events.

3.1.6 If an employee has any queries relating to the way in which Personal Information should be handled or Processed, then that employee should contact the Information Officer.

4. Conditions for lawful processing

4.1 We shall comply with the following conditions for the lawful Processing of Personal Information:

4.2 Personal Information must -

4.2.1 be processed lawfully and in a reasonable manner that does not infringe the privacy of the Data Subject;

4.2.2 be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the A2D24 that collects the Personal Information;

4.2.3 be adequate, relevant and not excessive in relation to the purpose for which the information is processed;

4.2.4 not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed;

4.2.5 be processed further only in accordance or compatible with the purpose for which it was collected;

4.2.6 collected and processed with the consent of the Data Subject, where required. In this context, consent refers to voluntary, specific and informed expression of will in terms of which permission is given for the Processing of Personal Information.

4.3 We shall–

4.3.1 take reasonably practicable steps to ensure that the Personal Information is complete, accurate, not misleading and updated where necessary;

4.3.2 maintain documentation of all Processing operations under our responsibility;

4.3.3 take reasonably practicable steps where Personal Information is collected to ensure that the Data Subject is aware of-

4.3.3.1 the information being collected and where the information is not collected from the Data Subject, the source from which it is collected;

4.3.3.2 the name and address of the Responsible Party (i.e. the A2D24 Entity which alone or in conjunction with others, determine the purpose of and means for processing Personal Information);

4.3.3.3 the purpose for which the information is being collected;

4.3.3.4 whether or not the supply of the information by that Data Subject is voluntary or mandatory;

4.3.3.5 the consequences of failure to provide the information;

4.3.3.6 any particular law authorising or requiring the collection of the information;

4.3.3.7 the fact that, where applicable, the Responsible Party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;

4.3.3.8 any further information such as the-

4.3.3.8.1 recipient or category of recipients of the information;

4.3.3.8.2 nature or category of the information;

4.3.3.8.3 existence of the right of access to and the right to rectify the information collected;

4.3.3.8.4 existence of the right to object to the Processing of Personal Information on reasonable grounds, unless legislation provides for such processing; and

4.3.3.8.5 right to lodge a complaint to a Regulator and the contact details of that Regulator (if any),

which is necessary, having regard to the specific circumstances in which the information is or is not to be Processed, to enable Processing in respect of the Data Subject to be reasonable.

4.4 Where we Process the Personal Information of a Data Subject on behalf of a client, the services agreement between A2D24 and the client shall provide that the client shall be responsible for obtaining consent from the Data Subject to process such Personal Information, and which consent shall include but not be limited to:

4.4.1 The collecting of the Data Subject's Personal Information;

4.4.2 transfer of data outside of SA; and or

4.4.3 request for removal or access to data.

4.5 Personal Information will only be Processed in accordance with the provisions of the services agreement between us and our client.

5. Special Personal Information

5.1 Special Personal Information relates to Personal Information concerning –

5.1.1 the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject; or

5.1.2 the criminal behaviour of a Data Subject to the extent that such information relates to the alleged commission by a Data Subject of any offence, or any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

5.2 We will only process Special Personal Information if the –

5.2.1 Processing is carried out with the consent of a Data Subject or A2D24 clients who have obtained such consent; or

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

5.2.3 Processing is necessary to comply with an obligation of international public law; or

5.2.4 Processing is for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned; or 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; or

5.2.5 information has deliberately been made public by the Data Subject.

5.3 Personal Information concerning a Data Subject's race or ethnic origin, may be processed, if the Processing is carried out to-

5.3.1 identify Data Subjects and only when this is essential for that purpose; and

5.3.2 comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

5.4 We understand the importance of protecting children's privacy especially in an online or technology-based environment. Our sites and products covered by this Policy are not intentionally designed for or directed at children 18 years of age or younger. It is A2D24's policy never to knowingly collect or maintain information about anyone under the age of 18.

6. Retention of Records

6.1 We understand that we have a statutory duty to keep certain records for a minimum period. We shall not keep Personal Information for longer than is necessary or as may be required by applicable law.

7. Security safeguards

Each Employee of A2D24 must –

7.1 secure the integrity and confidentiality of Personal Information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of Personal Information and unlawful access to or Processing of Personal Information;

7.2 take reasonable measures to-

7.2.1 identify all reasonably foreseeable internal and external risks to Personal Information in our possession or under our control;

7.2.2 establish and maintain appropriate safeguards against the risks identified;

7.2.3 regularly verify that the safeguards are effectively implemented; and

7.2.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards; and

7.2.5 have due regard to generally accepted Information Security practices and procedures which may apply generally or be required in terms of specific industry or professional rules and regulations.

8. Use of operators to process information

8.1 When we contract with third parties, we impose appropriate security, privacy and confidentiality obligations on them to ensure that Personal Information that we remain responsible for, is kept secure.

8.2 We may need to transfer Personal Information to another country for processing or storage. We will ensure that anyone to whom we pass Personal Information agrees to treat such information with the same level of protection as we are obliged to.

8.3 When subcontractors or other third parties (including cloud storage service providers) ("operators") are used to store or Process Personal Information on our behalf, we shall in terms of a written contract between ourselves and the operator, ensure that the operator which Processes Personal Information for A2D24, establishes and maintains the security measures referred to in 7 above.

8.4 The terms of the written contract must ensure that the operator notifies the relevant A2D24 Entity immediately where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person.

8.5 transborder information flows:

8.5.1 we shall not transfer Personal Information about a Data Subject to a third party who is in another country ("foreign country") unless-

8.5.1.1 the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection that-

8.5.1.1.1 effectively upholds principles for reasonable Processing of the information that are substantially similar to the conditions for the lawful processing of Personal Information relating to a Data Subject referred to in 4 above;

8.5.1.1.2 includes provisions, that are substantially similar to the provisions of this clause, relating to the further transfer of Personal Information from the recipient to third parties who are in a foreign country;

8.5.1.1.3 the Data Subject consents to the transfer;

8.5.1.1.4 the transfer is necessary for the performance of a contract between the Data Subject and A2D24, or for the implementation of pre-contractual measures taken in response to the Data Subject's request;

8.5.1.1.5 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between A2D24 and a third party; or

8.5.1.1.6 the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject to that transfer; and if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give it.

9. Information Security

9.1 We have implemented generally accepted standards of technology and operational security in order to protect personally identifiable information from loss, misuse, alteration or destruction.

9.2 All A2D24 employees follow a network-wide security policy. Only authorised A2D24 personnel are provided access to personally identifiable information and these employees have agreed to ensure confidentiality of this information.

9.3 We are legally obliged to provide adequate protection for the Personal Information we hold and to stop unauthorised access and use of Personal Information. We will, on an ongoing basis, continue to review our security controls and related processes to ensure that all Personal Information is secure.

9.4 Transmission of Data:

9.4.1 We shall ensure that all Personal Information communicated, including, any digital communication or any Personal Information stored in digital form shall be secured against being accessed or read by unauthorised parties, using appropriate security safeguards, having due regard to generally accepted Information Security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

10. Notification of a Personal Information Security Breach

We shall-

10.1 notify the Information Officer of the client in writing, immediately, of us becoming aware of or having reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by an unauthorised person and take all appropriate steps to limit the compromise of Personal Information and to restore the integrity of the affected information systems as quickly as possible;

10.2 as soon as reasonably possible thereafter, we shall engage with the client's Information Officer and any persons who may be appointed by the client to discuss the security breach, to report all relevant facts relating to the compromise and to accept directions from the client's Information Officer on steps to be taken to mitigate the extent of the compromise and loss occasioned by the compromise;

10.3 provide the client with details of the Personal Information affected by the compromise, including but not limited to, the identity of Data Subjects, the nature and extent of the compromise, and, where possible, details of the identity of the unauthorised person/s who are known to or who may reasonably be suspected of, having accessed or acquired the Personal Information;

10.4 immediately upon notifying the client as set forth in clause 10.1–

10.4.1 take all necessary steps as well as steps directed by the client's Information Officer to mitigate the continuation of the compromise, the repetition of a similar compromise, and mitigate the extent of the loss occasioned by the compromise of Personal Information;

10.4.2 implement all measures reasonably necessary to restore the integrity of our information system as quickly as possible;

10.4.3 provide the client's Information Officer with a report on its progress in resolving the compromise at reasonable intervals but at least once per business day following the initial notification to the client, until such time as the compromise is resolved to the client's and/or Information Officer's satisfaction;

10.4.4 if required by law, notify the South African Police Service and/or the National Intelligence Agency and cooperate with the client, South African Police Service and/or the National Intelligence Agency in the investigation of the cause of the compromise and the prosecution of person/s who may have gained or attempted to gain unauthorised access to or acquired Personal Information from us or the client; and

10.4.5 only upon request by the client, or otherwise if required by law, notify the Regulator and/or the affected Data Subjects. Any such notification shall be in a form prescribed by the client or the Regulator, as the case may be, if applicable and contain such information as is specified by the client. Notwithstanding the aforegoing, a notification to a Data Subject shall always include sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise.

11. Client's access to information

We shall –

11.1 assist the client to comply with any requests for access to Personal Information received by the client from Data Subjects and, at the request of the client, we shall promptly provide the client with a copy of any Personal Information held by us in relation to a specified Data Subject.

11.2 provide reasonable evidence of our compliance with our obligations under clause 9 to the client on reasonable notice and request;

11.3 at the request and option of the client, and to its satisfaction, promptly return or destroy all Personal Information in our possession or control, including in accordance with any specific retention, destruction and purging requirements as may be prescribed by the client; and

11.4 not Process the Personal Information otherwise than in accordance with this Policy.

11.5 In the event that we are required to disclose or Process any Personal Information required by law, regulation or court order, or if the Processing of such Personal Information is required to enable a public body to properly perform a public law duty to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party, is necessary for pursuing the legitimate interests of the client, a third party to whom the information is supplied, or a Data Subject, or complies with an obligation imposed by law on the client, we shall –

11.5.1 advise the client thereof prior to disclosure or Processing, if possible. If it is not possible to advise the client prior to disclosure or Processing, we shall advise the client immediately after such disclosure or Processing;

11.5.2 take such steps to limit the extent of the disclosure or Processing to the extent that we lawfully and reasonably practically can;

11.5.3 afford the client a reasonable opportunity, if possible and permitted, to intervene in the proceedings; and

11.5.4 comply with the client's requests as to the manner and terms of any such disclosure, if possible and permitted.

12. Separation of Personal Information

12.1 Unless otherwise specifically recorded any agreement or documents we shall not Process Personal Information provided by the client with, nor combine or merge such Personal Information with the information (whether Personal Information or not) of another party unless such combination or merging takes place for credit vetting purposes.

12.2 We shall endeavour to ensure that all authorised sub-contractors who Process Personal Information of Data Subjects shall not amend, modify, merge or combine such Personal Information.

13. Access to information

13.1 Any Data Subject shall have the right to request a copy of the Personal Information we hold about it by emailing support@a2d24.com; and

13.2 any such access request may be subject to a payment of a legally allowable fee.

14. Correction of personal information

14.1 Any Data Subject has the right to ask us to update, correct or delete its Personal Information, and may do so by emailing support@a2d24.com to make the request.

14.2 We will take all reasonable steps to confirm the identity of the Data Subject before making changes to Personal Information we may hold about such Data Subject.

14.3 We will encourage Data Subjects to keep their Personal Information accurate. Data Subjects may update their information by emailing support@a2d24.com whenever their details change.