



Date of first adoption: 19 May 2021  
Review and re-adoption: 23 September 2025

## PRIVACY POLICY OF THE DYKES VAN HEERDEN GROUP OF COMPANIES IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

### 1. INTRODUCTION

- 1.1 The Dykes van Heerden Group of Companies<sup>1</sup> (collectively referred to herein as “DvH”) Protection of Personal Information Policy and Compliance Manual (first adopted on 19May 2021) shall hereinafter be referred to as the “**the/this Policy**”, having been prepared in terms of the Protection of Personal Information Act 4 of 2013, as amended from time to time “**the Act**” and in terms of the Regulations thereto.
- 1.2 DvH as a Responsible Party is committed to protecting your privacy and to ensure that your personal information(hereinafter referred to as “**PI**”) is collected and used properly, lawfully and transparently. In terms of the Constitution, 1996 everyone has a right to privacy (section 14) which includes a right to protection against the unlawful collection, retention, dissemination, and use of PI.
- 1.3 This Policy explains how we obtain, use and disclose your PI, in accordance with the requirements of the Act, including what your right are.

Date/s of review and adoption		
Version 1 19 May 2021		Date of this Policy first unanimously adopted and approved by the directors of the Dykes van Heerden Group of Companies.
Version 2 23 September 2025		Date of review and amendments of this Policy, unanimously adopted and approved by all of the directors of the Dykes van Heerden Group of Companies.
Summary of amendments to the Regulations of POPIA		
1	Reg 2 Objection to the processing of personal information	<ul style="list-style-type: none"> <li>Various avenues for Data Subjects to object to their PI being processed. May submit the objection on a form <i>substantially similar</i> to Form 1 by hand, fax, post, email, SMS, or WhatsApp and/or in any manner expedient</li> <li>Duty to inform Data Subject of their right to object to processing</li> </ul>

<sup>1</sup> As at the date of these rules being adopted the Dykes van Heerden Group of Companies includes Dykes van Heerden Incorporated, Dykes van Heerden (Gauteng) Incorporated, Dykes van Heerden (Cape) Incorporated, Dykes van Heerden Slabbert Hopkins Incorporated, Dykes van Heerden (KZN) Incorporated.

		<ul style="list-style-type: none"> <li>• Telephonic objections: must be recorded electronically recorded</li> <li>• And made available to the Data Subject on request (if applicable)</li> </ul>
2	Reg 3 Request for correction or deletion of personal information or destruction or deletion of record of personal information	<ul style="list-style-type: none"> <li>• Data Subject requests for correction / deletion of or destruction / deletion of record of PI may be submitted on a form <i>substantially similar</i> to Form 2, by hand, fax, post, email, SMS, WhatsApp message or in any manner expedient to a Data Subject.</li> <li>• Obligation on Responsible Parties to notify the Data Subject of such correction, deletion or destruction</li> </ul>
3	Reg 4 Additional duties and responsibilities of Information Officer	<ul style="list-style-type: none"> <li>• Information Officers (IO's): continuous Improvement of the Compliance Framework: be maintained by IO's. Maintaining the PAIA Manual has fallen away.</li> </ul>
4	Reg 6 Request for a Data Subject's consent to process PI for direct marketing through unsolicited electronic communication.	<ul style="list-style-type: none"> <li>• On a form <i>substantially similar</i> to Form 4 / any expedient manner- includes fax, telephone, email, SMS, WhatsApp or automated calling machine (latter not applicable to DvH). Telephonic consent requirements – note: DvH does not record telephone calls.</li> </ul>
5	Reg 7 Who may lodge a complaint	<ul style="list-style-type: none"> <li>• “Complainant” has been defined under Definitions (paragraph 2)</li> </ul>
6	Reg 13 Administrative fines	<ul style="list-style-type: none"> <li>• May be paid in instalments</li> </ul>
7	Definitions	<ul style="list-style-type: none"> <li>• Addition of definitions for <i>complaint</i>, <i>complainant</i>, <i>office hours</i>, <i>days</i></li> </ul>

## 2. **DEFINITIONS**

- 2.1 **“the Act”** the Protection of Personal Information Act 4 of 2013 including its Regulations, as amended from time to time;
- 2.2 **“biometrics”** a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
- 2.3 **“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;
- 2.4 **“consent”** any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
- 2.5 **“Constitution”** the Constitution of the Republic of South Africa, 1996;
- 2.6 **“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;
- 2.7 **“complaint”** means-
- 2.7.1 a matter reported to the Information Regulator in terms of section 74(1) and (2) of POPIA;
- 2.7.2 a complaint referred to in section 76(1)(e) and 92(1) of POPIA; and

- 2.7.3 a matter reported or referred to the Information Regulator in terms of other legislation that regulates the mandate of the Information Regulator;
- 2.8 **"complainant"** any person who lodges a complaint with the Information Regulator and includes third parties, public interest actors, and proxies who may lodge complaints after which the Regulator will assist the complainant in one of the official languages of South Africa;
- 2.9 **"consent"** any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
- 2.10 **"Data Subject"** the person (natural person or a juristic person) to whom the personal information relates;
- 2.11 **"day"** a calendar day, unless the last day of a specified period happens to fall on a Sunday or on any public holiday, in which case the time shall be calculated exclusive of that Sunday or public holiday in accordance with section 4 of the Interpretation Act 33 of 1957;
- 2.12 **"de-identify"** in relation to personal information of a Data Subject, means to delete any information that—
- 2.12.1 identifies the Data Subject; or
  - 2.12.2 can be used or manipulated by a reasonably foreseeable method to identify the Data Subject; or can be linked by a reasonably foreseeable method to other information that identifies the Data Subject, and "de-identified" has a corresponding meaning;
- 2.13 **"direct marketing"** contacting the Data Subject directly or indirectly via electronic communication for the purpose of promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject;
- 2.14 **"electronic communication"** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;
- 2.15 **"enforcement notice"** a notice issued in terms of section 95 of POPIA;
- 2.16 **"filing system"** any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;
- 2.17 **"Information Officer"/"IO"** of, or in relation to, a private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;
- 2.18 **"Minister"** means the Cabinet member responsible for the administration of justice;

- 2.19 **“office hours”** in respect of offices of the Information Regulator, means the hours between 08:00 and 16:00 on Monday to Friday, excluding public holidays, and in respect of offices designated by the Information Regulator, means the hours during which the offices are operating;
- 2.20 **“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;
- 2.21 **“office hours”** in respect of offices of the Information Regulator, means the hours between 08:00 and 16:00 on Monday to Friday, excluding public holidays; and in respect of offices designated by the Information Regulator, means the hours during which the offices are operating;
- 2.22 **“PAIA”** the Promotion of Access to Information Act 2 of 2000;
- 2.23 **“personal information / PI”** personal information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
- 2.23.1 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;
  - 2.23.2 information relating to the education or the medical, financial, criminal or employment history of the person;
  - 2.23.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
  - 2.23.4 the biometric information of the person;
  - 2.23.5 the personal opinions, views or preferences of the person;
  - 2.23.6 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;
  - 2.23.7 the views or opinions of another individual about the person; and
  - 2.23.8 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;
- 2.24 **“POPIA”** the Protection of Personal Information Act 4 of 2013, amended from time to time / the POPI Act;

- 2.25 **“processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
- 2.25.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
  - 2.25.2 dissemination by means of transmission, distribution or making available in any other form; or
  - 2.25.3 merging, linking, as well as restriction, degradation, erasure or destruction of information;
- 2.26 **“public record”** a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;
- 2.27 **“record”** any recorded information regardless of form or medium, including any of the following-
- 2.27.1 writing on any material;
  - 2.27.2 information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
  - 2.27.3 label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
  - 2.27.4 book, map, plan, graph or drawing;
  - 2.27.5 photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
  - 2.27.6 in the possession or under the control of a Responsible Party; whether or not it was created by a Responsible Party and regardless of when it came into existence;
- 2.28 **“Regulator”** the Information Regulator established in terms of section 39 of POPIA;
- 2.29 **“relevant body”/“bodies”** refers to any specified body or class of bodies, or any specified industry, profession, or vocation or class of industries, professions, or vocations that in the opinion of the Regulator which has sufficient representation;
- 2.30 **“the 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; and
- 2.31 **“writing”** writing as referred to in section 12 of the Electronic Communication and Transaction Act 25 of 2002.

### 3. THE PURPOSE OF THE POPI ACT

- 3.1 In terms of section 14 the Constitution, 1996, everyone has a right to privacy which includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.
- 3.2 The purpose of POPIA is to, amongst others, regulate, in harmony with international standards, the processing of personal information of people and entities (referred to as “**Data Subjects**”) by public and private bodies (called “**Responsible Parties**”) in a manner that gives effect to the right to privacy.
- 3.3 Privacy is a constitutional right but is not absolute can be limited in situations where other important rights come into play, such as the right to freedom of expression or the public’s right to know. Courts balance these competing rights to decide whether privacy should be protected in each case.
- 3.4 DvH and each firm within the group is deemed to be a registered Responsible Party, which processes personal information of Data subjects (including but is not limited to the personal information of current and past clients, current and past employees and service providers, to name a few). Each firm within the DvH Group of Companies is registered with the Information Regulator, which is an independent body established in terms of section 39 of POPIA.

### 4. WHAT IS PERSONAL INFORMATION?

- 4.1 Personal information is defined very broadly as an identifiable, living, natural person’s information and, where applicable, an identifiable, existing juristic person’s information, including, but not limited to:
  - 4.1.1 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;
  - 4.1.2 information relating to the education or the medical, financial, criminal or employment history of the person;
  - 4.1.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
  - 4.1.4 the biometric information of the person;
  - 4.1.5 the personal opinions, views or preferences of the person;
  - 4.1.6 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;
  - 4.1.7 the views or opinions of another individual about the person; and
  - 4.1.8 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.

- 4.2 Examples of a juristic entity's personal information include but is not limited to –
  - 4.2.1 information relating to the ownership (for example black owned);
  - 4.2.2 age (for example been registered for ten years) including
    - 4.2.2.1 financial data of the entity;
    - 4.2.2.2 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature; or
    - 4.2.2.3 further correspondence that would reveal the contents of the original correspondence
    - 4.2.2.4 information relating to the education or the medical, financial, criminal or employment history of the person.
- 4.3 Special personal information<sup>2</sup> is the sensitive class of personal information and a Responsible Party may not, subject to section 27, process personal information concerning 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 the criminal behaviour of a Data Subject to the extent that such information relates to—
  - 4.3.1.1 the alleged commission by a Data Subject of any offence; or
  - 4.3.1.2 any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

## 5. **RIGHTS OF DATA SUBJECTS (SECTION 5)**

In terms of POPIA certain rights are given to Data Subjects (being the person to whom personal information relates). These rights include:

- 5.1 **Notification of the information being collected and for what purpose;**
- 5.2 **Establishing what information the Responsible Party holds and the right to request access to such information;**
- 5.3 **Object to the processing<sup>3</sup> of his/her information**
  - 5.3.1 A Data Subject who wishes to object to the processing of their PI and to direct marketing, must submit the objection to the Responsible Party on a form substantially similar to Form 1, free of charge and reasonably accessible by hand, fax, post, email, SMS, or WhatsApp and or in any manner expedient to a Data Subject.;
  - 5.3.2 When collecting the PI, the Responsible Party has a duty to inform the Data Subject of their right to object to processing their PI.
  - 5.3.3 If an objection is made telephonically, such an objection shall be electronically recorded by the Responsible Party and made available to the Data Subject on request, for free.
  - 5.3.4 Objections may be lodged at any time during normal working hours and may be lodged through various channels, including telephonically.
- 5.4 **Request correction, deletion or destruction of personal information**

---

<sup>2</sup> Section 26 of POPIA

<sup>3</sup> Regulation 2 of POPIA- *Objection to process personal information*

- 5.4.1 At no additional cost, Data Subjects may use Form 2 (Request For Access To Record) or a form *substantially similar* to Form 2, to exercise this right.
- 5.4.2 Multiple channels now includes telephonic communication, which may be used by the Data Subject to request for the correction, destruction or deletion of P in the event of the Responsible Party is no longer being authorised to retain such data.
- 5.5 Responsible Parties have 30 days after *receipt of the outcome* to inform the Data Subject in writing of any action taken in terms of the request.

## 6. **CONDITIONS OF LAWFUL PROCESSING – CHAPTER 3 OF THE POPI ACT**

- 6.1 POPIA provides for the establishment of minimum requirements for processing of personal information. The conditions for lawful processing of personal information which consist of eight conditions, which will be dealt with as necessary in more detail in this Policy, namely:

- 6.1.1 Condition 1 - Accountability;
- 6.1.2 Condition 2 - Processing limitation;
- 6.1.3 Condition 3 - Specific purpose;
- 6.1.4 Condition 4 - Further processing limitation;
- 6.1.5 Condition 5 - Information quality;
- 6.1.6 Condition 6 - Openness;
- 6.1.7 Condition 7 - Security safeguards;
- 6.1.8 Condition 8 - Data subject participation.

### 6.2 **Accountability – Condition 1**

- 6.2.1 The Responsible Party is held accountable for ensuring that the personal information processing is done in a lawful, responsible, and ethical manner, in line with POPIA.
- 6.2.2 If the Data Subject does not consent to the processing and storage of some of their information on the or refuses and/or opts out of receiving direct marketing, this will be recorded and DvH's database. It should be noted, however, that DvH may not be able to carry out the instruction if the Data Subject who does not consent to the processing of certain personal information is necessary for DvH to successfully render the services.

### 6.3 **Processing Limitations – Condition 2**

- 6.3.1 Section 11(1) of POPIA provides that personal information may only be processed if—
  - 6.3.1.1 the Data Subject or a competent person where the Data Subject is a child consents to the processing;
  - 6.3.1.2 processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is party;
  - 6.3.1.3 processing complies with an obligation imposed by law on the Responsible Party;
  - 6.3.1.4 processing protects a legitimate interest of the Data Subject;



- 6.3.1.5 processing is necessary for the proper performance of a public law duty by a public body; or
- 6.3.1.6 processing is necessary for pursuing the legitimate interests of the Responsible Party or of a third party to whom the information is supplied.
- 6.3.2 The personal and special personal information collected should be adequate, relevant and not excessive, for the purposes of complying with the obligations of the FIC Act and based on the instruction given to DvH from the Data Subject.
- 6.3.3 The PI obtained will be stored –
  - 6.3.3.1 by each firm in the DvH Group on its own electronic database which may include physical copies/originals and a signed consent form, or
  - 6.3.3.2 in the any other accessible form. In terms of consent, POPIA Regulations now provide that telephonic consent may be given by the Data Subject (however, DvH does not, as this stage, record telephonic discussions).

#### 6.4 **Purpose Specification – Condition 3**

- 6.4.1 The personal information of the client may be retained for birthday notifications, anniversary notifications and/or for marketing (if consented to).
- 6.4.2 The condition purpose specification means that the Responsible Party may only collect personal information for specific, clearly defined, and legitimate reasons that are related to the Responsible Party's functions or activities, as stated in section 11 of POPIA.
- 6.4.3 This is requirement is to ensure that the Responsible Party remains transparent by informing Data Subjects why their data is being collected and processed, allowing Data Subjects to control how their information is being used and preventing processing for unrelated purposes.
- 6.4.4 Personal information, which is stored by the Responsible Party, must be deleted / destructed if the Data Subject requests the destruction or deletion thereof, depending on the laws applicable to the personal information which the Data Subject has requested be destroyed and which is being retained by the Responsible Party.
- 6.4.5 The POPI Act requires records to be kept only as long as necessary for the purpose for which they were collected, unless a law requires a longer period. For example, the Companies Act 71 of 2008 requires that records be kept for 7 years. Once the purpose is no longer valid, the Responsible Party should destroy, delete, or de-identify the information, unless a law provides an exception.

#### 6.5 **Further Processing Limitation – Condition 4**

- 6.5.1 POPIA provides that further processing of PI must be in accordance or compatible

- with the purpose for which it was collected (the original purpose)
- 6.5.2 If further processing is not for purposes for which it was obtained and there is no valid justification (such as public interest). consent would be required from the Data Subject again.
- 6.5.3 When determining if further processing is compatible, the Responsible Party will consider–
- 6.5.3.1 the type of personal data being processed;
  - 6.5.3.2 the connection between the initial purpose and the new purpose of processing;
  - 6.5.3.3 how the further processing might affect the individual;
  - 6.5.3.4 manner in which the information was originally obtained; and any existing contractual relationships between the parties involved.
- 6.5.4 Therefore further processing is permissible if (including but not limited to)–
- 6.5.4.1 the Data Subject provides consent;
  - 6.5.4.2 the information is publicly available; or
  - 6.5.4.3 it is necessary in terms of public interest ( for example preventing threats to public health or for historical, statistical, or research purposes).

## **6.6 Information Quality – Condition 5**

The Information Officer of the relevant DvH firm will take all reasonable steps to ensure that the information uploaded to the relevant physical and/or electronic databases are complete and accurate and are updated where necessary. Information should not have missing details which are necessary relevant to the purpose of collection and must reflect the true state of affairs.

## **6.7 Openness – Condition 6**

- 6.7.1 Data Subjects must be made aware of certain information when their consent is being obtained, this is specified in the DvH Consent Form and should be pointed out by staff to the client / Data Subject when the relevant form is signed, or should another method be used to obtain consent. The Data Subject must be made aware that they can object to the further processing.
- 6.7.2 Subject to the FIC Act and other applicable legislation, the Data Subject may at any time withdraw his/her consent at which time they shall be removed from the relevant database / marketing database for further processing.

## **6.8 Security Safeguards– Condition 7**

- 6.8.1 DvH must 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 –
- 6.8.1.1 loss of, damage to or unauthorised destruction of personal information; and/or
  - 6.8.1.2 the unlawful access to or processing of personal information.

- 6.8.2 In order to safeguard data and personal information, DvH safeguards include but is not limited to:
- 6.8.2.1 physical measures (for example, securing filing cabinets and access control at offices);
  - 6.8.2.2 organisational measures (for example training staff on the importance of protecting personal information);
  - 6.8.2.3 technological measures (for example, implementing firewalls and anti-virus programmes, using passwords and encrypting removable devices used for taking personal information out of the office); and
  - 6.8.2.4 the development of an information security policy for privacy which addresses all of the above and checking that DvH's nominated service providers / operators that complies with the obligation of ensuring security safeguards are in place whilst assisting DvH it in its business operations.
- 6.8.3 In the event of f personal information accessed or acquired by any unauthorised person the nominated Information Officer / Deputy Information Officer must notify the Information Regulator and the Data Subjects who may be affected as soon as reasonably possible.

## 6.9 **Data Subject Participation – Condition 8**

- 6.9.1 Data subjects can exercise their rights related to their personal information. This is achieved through several key rights: right to be informed, right to access their personal information held by a Responsible Party, right to correction, and to object to the processing of their personal information.
- 6.9.2 Depending on specific interpretations of the law, Data Subjects may also request the deletion / destruction of their personal Information, subject to certain other laws (of applicable).
- 6.9.3 Data Subjects may object to receiving unsolicited direct marketing and may only be contacted once by electronic communication for direct marketing purposes from companies/entities, during which the Data Subject may request that no further direct marketing be sent to him/her.
- 6.9.4 On request from a client subject DvH and the nominated Information Officer shall as soon as reasonably possible correct, destroy or delete the personal information.

## 7. **DIRECT MARKETING**

- 7.1 DvH does not send direct marketing by electronic means, which includes SMS, e-mails, telemarketing calls, telephone calls from people, SMS's andWhatsapps, to Data Subjects at this stage.

- 7.2 Notwithstanding the contents of clause 7.1 and the fact that DvH does not usually send direct marketing in the normal course of conducting its business, should DvH ever process personal information for purposes of sending direct marketing to potential or current clients, it shall do so in accordance with the provisions of POPIA, considering the Data subject's preferences.
- 7.3 The Data subject may refuse processing for direct marketing by unsolicited electronic communications or complain to the Information Regulator and institute civil proceedings. DvH does not send direct marketing to Data Subjects in the ordinary course of running its business however, in the event that DvH may do so, for whatever reason, it shall as a Responsible Party ensure that express and clear consent is given by the Data Subject.
- 7.4 DvH will also ensure that the Data Subject is fully aware of the purpose of the marketing, the types of goods or services, and the method of communication it may choose (e.g., email, SMS). either by –
- 17.1.1 obtaining consent in written form through a Form substantially similar to Form 4, or in any expedient way;
  - 17.1.2 telephonic consent or automated calling machines;
  - 17.1.3 providing opportunities to opt-out, but it must be noted that opting-out may not be considered as consent to direct marketing.<sup>4</sup> and
  - 17.1.4 may only approach a Data Subject once to request initial consent for electronic direct marketing.
- 17.3 Data subject can choose their preferred communication method, such as telephone calls, email or SMS, and the marketer/Responsible Party must obtain and respect this choice.

## 8. **INFORMATION OFFICERS AND DEPUTY INFORMATION OFFICERS**

- 8.1 The directors of each office of DvH are responsible for ensuring compliance with POPIA including this Policy by the staff of each such office. The obligation on information officers to prepare PAIA Manuals has been deleted however Information Officers must still ensure that a compliance framework is developed, implemented, monitored, maintained and continually improved.
- 8.2 In order to assist the directors with discharging their duties, the following nominated Information Officers and deputy Information Officer set out below are appointed by each office to support and report to the directors.
- 8.3 Any and all assistance required in implementing the Policy, or concerns arising regarding potential and existing clients / Data Subject queries should be escalated to the nominated Information Officer and Deputy Information Officer.
- 8.4 A Data Subject who wishes to request a correction, deletion or destruction of PI must submit the request to a Responsible Party on a form substantially similar to Form 2, free of charge and reasonably accessible to a Data Subject by hand, fax, post, email, SMS, WhatsApp message or in any manner expedient to a Data Subject.

---

<sup>4</sup> Regulation 6 of the Popi Act

<b>Branch</b>	<b>DvH Inc - Bonds</b>	<b>DvH (Cape) Inc- Bonds</b>	<b>DvH (KZN) Inc</b>
	<b>DvH (Gauteng) Inc - Transfers</b>	<b>DvH Slabbert Hopkins Inc - Transfers</b>	
<b>Office Address</b>	18Ontdekkers Road Roodepoort Gauteng 1724	120-122 Edward Rd Cape Town 7530	76 Old Main Road Kloof 4124
<b>Postal Address</b>	Docex 24, Roodepoort	Docex 42, Tygerberg	Docex 7, Amanzimtoti
<b>Office Tel: Office Fax:</b>	(011) 279 5000	(021) 910 1911	(031) 101-3081 (031) 903-1101
<b>Information Officer</b>	Herbert James Robertson (JD)	Elena Hopkins	Thomas van Heeswijk
<b>E-mail</b>	<a href="mailto:jd@dvh.za.net">jd@dvh.za.net</a>	<a href="mailto:elanah@dvh.law.za">elanah@dvh.law.za</a>	<a href="mailto:Thomas@dvhlaw.co.za">Thomas@dvhlaw.co.za</a>
<b>Mobile:</b>	+27 71 372 6555	+27 82 928 3041	+27 82 353 5849
<b>Deputy Information Officer</b>	Zinhle Mbali Keitumetse Sibisi (Mbali).	Carmen Nieman	Lisa Boniface
<b>E-mail:</b>	<a href="mailto:Mbali@dvh.za.net">Mbali@dvh.za.net</a>	<a href="mailto:carmenn@dvh.law.za">carmenn@dvh.law.za</a>	<a href="mailto:lisa@kzndvh.za.net">lisa@kzndvh.za.net</a>
<b>Cell:</b>	+27 71 011 2049 (Note: no Whatsapp on this number)	TBC / alternatively (021) 910 1911	+27 83 414 4817

## 9. THE INFORMATION REGULATOR AND COMPLAINTS

- 9.1. Any person who wished to submit a complaint must submit such complaint to the Information Regulator using Form 5 or
- 9.2. The following persons may lodge a complaint against a Responsible Party:
- 9.2.1. Data Subject whose PI has been interfered with,
  - 9.2.2. any person acting on behalf of a Data Subject whose PI has been interfered with,
  - 9.2.3. any person with a sufficient personal interest in the complaint,
  - 9.2.4. a Responsible Party of Data Subject aggrieved by the determination of an adjudicator, or
  - 9.2.5. any person acting in the public regarding the Policy or any personal information matters which it wants to report.
- 9.3 The details of the Information Regulator:
- 9.3.1 Address : Woodmead North Office Park, 54 Maxwell Dr, Woodmead, Sandton, 2191
  - 9.3.2 Phone: 010 023 5200

- 9.3.3 E-mail: [enquiries@inforegulator.org.za](mailto:enquiries@inforegulator.org.za) or [POPIAComplaints@inforegulator.org.za](mailto:POPIAComplaints@inforegulator.org.za)
- 9.3.4 Website : <https://inforegulator.org.za/>

## **10. TRAINING**

- 10.1 Training and the manner thereof of staff and will be in the discretion of management of each firm within the Group and may be conducted by way of:
  - 10.1.1 a presentation involving the entire staff complement of employees and administrative personnel and for all new staff in each group of companies forming part of DvH;
  - 10.1.2 in group sessions, when importance changes occur and as frequently as the board of directors may direct.
- 10.2 Training and individual refresher training will also be available to employees on request.
- 10.3 Each staff member will be provided with a copy of the Policy as revised from time to time and may be required to sign an acknowledgement of receipt and an acknowledgement that training has been effected.

## **11. NON-COMPLIANCE AND PENALTIES FOR NON-COMPLIANCE**

- 11.1 Compliance will be enforced by an Information Regulator, which will have far-reaching powers. POPIA provides for the following penalties for non-compliance (depending on severity):
  - 11.1.1 3 months' to ten years' imprisonment;
  - 11.1.2 administrative fines of up to ZAR 10 million;
  - 11.1.3 civil action from Data Subjects for damages; and
  - 11.1.4 severe reputational harm.
- 11.2 These penalties are imposed by the Information Regulator for offenses such as failing to implement reasonable security measures to protect personal data or obstructing its enforcement activities.
- 11.3 Administrative fines<sup>5</sup> which the Information Regulation, at its discretion, may allow be paid by the Responsible Party being fines, in instalments. A Responsible Party served with an infringement notice by the Information Regulator for committing an offence in terms of POPIA and who is unable to pay the administrative fine in a lump sum, may decide with the Information Regulator to pay the administrative fine in instalments on a case-by-case basis.
- 11.4 When determining an appropriate payment period, the Information Regulator must consider the financial circumstances of the Responsible Party, and any other relevant compelling reasons that may directly or indirectly impact on the Responsible Party's affordability.
- 11.5 Failure by any employee to comply with this Policy will constitute a breach of such employee's conditions of employment, and may therefore expose such employee to disciplinary procedures, or may expose the staff member and DvH to criminal penalties which are severe. In the event of non-compliance, alleged or suspected non-compliance with POPIA

---

<sup>5</sup> Administrative fines are based on the POPIA Regulation amendments effective 17 April 2025

and this Policy a disciplinary hearing will be held and non-compliance could result in dismissal.

<b>Adoption of this Privacy Policy: version 2</b>	<b>23 September 2025</b>
---	--------------------------

We, the nominated Information Officers of each of the firms forming part of the DvH Group of companies, hereby confirm that this updated Privacy Policy is officially adopted as the Group's Privacy Policy. All representatives and staff are required to familiarise themselves with this Policy, and to comply.



---

**Herbert James Robertson**



---

**Elena Hopkins**



---

**Thomas van Heeswijk**