RAATH ATTORNEYS

DATA BREACH AND RESPONSE POLICY

PREPARED IN ACCORDANCE WITH SECTION 22 OF THE

RAATH ATTORNEYS: PROPERTY DIVISION
4B Faraday Blvd. Vanderbijlpark, 1911
Mobile Number: +27 74 242 5000
Website: www.gwraath.co.za

PROTECTION OF PERSONAL INFORMATION ACT, NO. 4 OF 2013 ("POPIA")

TABLE OF CONTENTS

1. **INTRODUCTION**

1.1 Section 22 of the **PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013** ("POPIA") requires RAATH ATTORNEYS to secure the integrity and confidentiality of Personal Information in their possession.

1.2 It is important to remember that POPIA is in effect from **01 JULY 2020**, withthe exception of certain provisions coming into force on **30 JUNE 2021**, andthat RAATH ATTORNEYS have until 01 July 2021 to become POPIA compliant,before **SANCTIONS** and **PENALTIES** apply.

1.3 POPIA focusses on the processing of Personal Information, and sets new **RULES** for regulating Personal and Special Personal Information.

1.4 RAATH ATTORNEYS are compelled to secure the **INTEGRITY** and **CONFIDENTIALITY** of Personal Information in their possession and a **DATA BREACH DOES** fall within the ambit of the legal framework established by POPIA and businesses have certain obligations in this regard.

2. **ACTION ON DATA BREACH**

2.1 In terms of section 22 of POPIA, where there are **reasonable grounds** to believe that the personal information of a data subject (customer or employee) has been accessed or acquired by any unauthorized person, the **RESPONSIBLE PARTY** must notify the **INFORMATION REGULATOR, INFORMATION OFFICER AND THE DATA SUBJECT**, unless the identity of such data subject cannot be established.

2.2 The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

2.3 The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Information Regulator determines that notification willimpede a criminal investigation by the public body concerned, if not, the notification must be in writing and communicated to the data subject in a prescribed manner.

2.4 Any suspicion, on reasonable grounds, that personal information has been accessed or acquired by an unauthorised person must be reported to both the

data subject and the Information Regulator. This notification must be inwriting, and must provide sufficient information to allow the data subject totake protective measures.

2.5 The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including all of the following:

2.5.1 A description of the possible consequences of the security compromise

2.5.2 A description of the measures that the responsible party intends totake or has taken to address the security compromise

2.5.3 A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the securitycompromise

2.5.4 If known to the responsible party, the identity of the unauthorized person who may have accessed or acquired the personal information

2.5.5 The notice must be communicated to the data subject concerned inany one of the following ways:

2.5.6 By post to the last known physical or postal address of the datasubject;

2.5.7 By email to the last known e-mail address of the data subject;

2.5.8 Placed in a prominent position on the website of the responsibleparty;

2.5.9 Published in the news media;

2.5.10 Communicated in any other manner as directed by the InformationRegulator.

3. **INFORMATION REGULATOR**

3.1 The Information Regulator may direct a responsible party to publicize, in any manner specified, the fact of any compromise to the integrity orconfidentiality of personal information, if the Information Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

3.2 An operator / data processor is not required to notify the Information Regulator

or data subjects where there are reasonable grounds to believe that there has been a data breach. It must, however, notify the responsibleparty/data controller of the suspected data breach.

4. DATA BREACHES

4.1 POPIA does not define **DATA BREACHES**, but it is clear that a Data Breach has occurred when there are reasonable grounds to believe that any **UNAUTHORISED PERSON** has accessed or acquired Personal Information under the control of BRENNER BRANDS, or if data has been intentionally or **ACCIDENTLY LOST**, **SHARED** or **DESTROYED.**

4.2 **DATA BREACHES** may occur in different ways, including but not limited to **HACKING**, **THEFT**, **ACCIDENTAL LOSS** and **UNAUTHORISED USE** of Personal Information and a data breach can take place through either through **PHYSICAL BREACH** or **ELECTRONIC BREACH**.

4.3 Theft of a Laptop containing Personal Information or potential Personal Information will constitute a serious **DATA BREACH** subject to sanction in terms of POPIA.

5. IT ACTIONS AND SECURITY

5.1 Ensure hard copies of data subject information are stored securely in locked filing cabinets or rooms. Data Subject files should never be left unattended on a reception counter of a busy offices.

5.2 All computer screens should not be visible to the data subjects and general public.

5.3 Be aware of browser and cookie settings which should not be allowed as to limit trace.

5.4 Passwords should never be saved on the computer or written down in prominent places. Passwords should comply with the difficulty grades as recommended by the BRENNER BRANDS IT advisors and changed on regular basis.

5.5 Only use the installed computers within the RAATH ATTORNEYS offices and do not store Personal Information on Laptops!

5.6 The Responsible Party is required to consider its options to limit the potential adverse consequences of the breach in case of a laptop theft. Should you be able to remotely wipe the laptop, or track such or enable **encryption**, such options should be considered. At all times follow the recommendations of RAATH ATTORNEYS IT Department.

5.7 Under the terms of POPI, the arrangements around third party access to Data Subject information requires Data Subject consent in most situations.

6. NON COMPLIANCE WITH POPI

6.1 Failure to observe and comply with the provisions of POPI can lead to a variety of implications for RAATH ATTORNEYS – some of which are potentially very serious. These are:

6.2 A complaint lodged with the Information Regulator

6.3 Receiving a civil claim for payment of any damages;

6.4 Criminal prosecution – if convicted there could be a fine up to R10 million or a prison sentence up to ten years, or even both.

7. CONTACT DETAILS OF MANAGING DIRECTOR

NAME	Gideon Raath
CONTACT NUMBER	+27 74 242 5000
EMAIL ADDRESS	sales@gwraath.co.za
WEB SITE:	www.gwraath.co.za
PHYSICAL ADDRESS:	4B Faraday Blvd. Vanderbijlpark, 1911
POSTAL ADDRESS:	Same as above

8. **CONTACT DETAILS OF THE INFORMATION OFFICER**

NAME	Gideon Raath
CONTACT NUMBER	+27 74 242 5000
EMAIL ADDRESS	sales@gwraath.co.za
WEB SITE:	www.gwraath.co.za
PHYSICAL ADDRESS:	4B Faraday Blvd. Vanderbijlpark, 1911
POSTAL ADDRESS:	Same as above

9. **CONTACT DETAILS OF INFORMATION REGULATOR**

INFORMATION REGULATOR ADV PANSY HLAKULA
Email: Complaints.IR@justice.gov.za
Website: htttp://www.justice.gov.za/inforeg/
JD House, 27 Siemens Street, Braamfontein, Johannesburg