

# DATA PROTECTION POLICY

DE UIJLENES WEDDINGS (PTY) LTD

De  
UIJLENES

De  
UIJLENES  
FOREST & BARN WEDDINGS



## **TABLE OF CONTENTS**

1. INTRODUCTION AND BACKGROUND .....	3
2. DEFINITION TERMS .....	3
3. POLICY PURPOSE .....	7
4. POLICY SCOPE AND APPLICATION.....	8
5. POLICY PRINCIPLES .....	8
6. WHEN IS DATA ALLOWED TO BE PROCESSED .....	10
7. DATA BREACH.....	10
8. TERM.....	11
9. RULES IN TERMS OF THIS POLICY .....	11
10. DATA SUBJECT ACCESS REQUESTS .....	13
11. ENQUIRY PROTOCOL AND GUIDELINES .....	13
12. BREACH OF THIS POLICY .....	14
13. REVIEW, MONITORING AND EVALUATION OF THE POLICY .....	15

## 1. INTRODUCTION AND BACKGROUND

- 1.1. The right to privacy is an important human right entrenched and protected by the Protection of Personal Information Act 4 of 2013 and the General Data Protection Regulation 2016/679
- 1.2. De Uijlenes Weddings (Pty) Ltd recognizes the importance of privacy and is committed to handling the personal information of customers, employees and third party personnel in accordance with the provisions of the Protection of Personal Information Act 4 of 2013 and the General Data Protection Regulation 2016/679.
- 1.3. This is the main Data Protection Policy for De Uijlenes Weddings (Pty) Ltd.

## 2. DEFINITION TERMS

- 2.1 In this Policy, the following words shall, unless otherwise stated or inconsistent with the context in which they appear, bear the following meanings and other words derived from the same origins as such words (that is, cognate words) shall bear corresponding meanings:
  - 2.1.1 "**Associated Persons**" means the Company's Employees and Persons.
  - 2.1.2 "**Biometrics**" means a technique of personal identification that is based on physical, physiological or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
  - 2.1.3 "**Commencement Date**" means the date upon which this Policy will come into force being \_\_\_\_\_.
  - 2.1.4 "**Company**" means **De Uijlenes Weddings (Pty) Ltd**, with registration number: 2012/168693/07, and having its registered address at Uilkraal Farm, Gansbaai, Western Cape, 7220, and including but not limited to all affiliates, subsidiaries, related and inter-related parties.
  - 2.1.5 "**Consent**" means voluntary, specific, informed expression of will in terms of which permission is given to process personal information.
  - 2.1.6 "**Data Protection Officer**" means the Company's designated employee who supervises, monitors and reports on compliance with this Policy.

2.1.7 "**Data Subject**" means a natural or juristic person to whom the Personal Data relates and whose data is processed.

2.1.8 "**Employee**" means any employee duly employed by the Company on a fixed term or permanent basis.

2.1.9 "**Filing System**" means any structured set of personal information, in a centralized, decentralized or dispersed basis, which is arranged according to specific criteria.

2.1.10 "**GDPR**" means the General Data Protection Regulation 2016/679.

2.1.11 "**Interim Period**" means the period of 3 (three) years from the Commencement Date.

2.1.12 "**Personal Data**" means any non-public personal information collected directly from the Data Subject which can directly or indirectly identify such Data Subject including but not limited to the following:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, color, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of the person;
- medical, financial, criminal or employment history of a person;
- any identifying name, number, symbol, email address, physical address, telephone number, location information, online identifier;
- biometric information of the person;
- personal opinions, views or preferences of a person, or of another person about the person; and
- correspondence of a private or confidential nature, whether implicit or explicit, or would reveal the contents of data.

2.1.13 "**Persons**" means all service providers who have entered into a contractual relationship with the Company for the supply of goods and/or services and any other relevant external parties engaged with the Company in their professional and/or personal capacity, which is not provided for above.

2.1.14 "**Policy**" means this document, including any schedules and annexures attached hereto, as amended from time to time.

2.1.15 "**POPIA**" means the Protection of Personal Information Act 4 of 2013, as amended, and including all annexures and regulations thereto.

2.1.16 "**Record**" means recorded information in any form, including, without limitation, writing, tape recorder, computer equipment (hardware/software), or other electronic device from which information may be stored, derived, produced or recorded; label, marking, book, map, plan, graph, drawing, photograph, film, negative, tape, or any other device in which a visual image may be embodied and reproduced.

2.1.17 "**Responsible Party / Parties**" means the person(s) that requires the Personal Data for any particular reason and determines the purpose of and means for processing the Personal Data.

2.2 In this Policy, unless the context clearly indicates a contrary intention, the following will apply:

2.2.1 Clause headings are for convenience and shall not be used in its interpretation.

2.2.2 An expression which denotes any gender includes the feminine and neuter genders and vice versa.

2.3 Where:

2.3.1 a number of days is prescribed, it shall consist of any days of the week including Saturdays, Sundays and public holidays (recognized in South Africa) and shall be calculated exclusively of the first and inclusively of the last day;

2.3.2 a day upon which any act is required to be performed is not a business day, the Parties shall be deemed to have intended such act to be performed upon or by the first business day thereafter; and

2.3.3 figures are referred to in numerals and words, the words shall prevail in the event of a conflict between the two.

2.4 Any reference to:

2.4.1 the singular shall include the plural and vice versa;

- 2.4.2 a natural person shall include bodies corporate, trusts and other legal personae and vice versa;
- 2.4.3 an enactment is to that enactment as at the date of signature and as amended, replaced or re-enacted from time to time;
- 2.4.4 a document or instrument includes the document or instrument as ceded, delegated, novated, altered, supplemented or replaced from time to time; and
- 2.4.5 to a Party includes that Party's successors-in-title and permitted assigns.
- 2.5 If any provision in a definition is a substantive provision conferring rights or imposing obligations on any Party, notwithstanding that it is only in the definition clause, effect shall be given to it as if it were a substantive provision in the body of this Policy.
- 2.6 Expressions defined in this Policy shall bear the same meanings in schedules or annexures to this Policy which do not themselves contain their own definitions.
- 2.7 All schedules and annexures hereto shall be deemed to form part of this Policy and in any instance where there is a conflict between a provision (be it expressed, implied or tacit) of this Policy and a provision of an annexure or schedule to this Policy, the provision of this Policy shall prevail.
- 2.8 Where any term is defined within the context of any particular clause in this Policy, the terms so defined, unless it is clear from the clause in question that the terms so defined has limited application to the relevant clause, shall bear the meaning ascribed to it for all purposes in terms of this Policy, notwithstanding that the term has not been defined in this interpretation clause.
- 2.9 The use of the word "including", "includes", "include" and "in particular", followed by a specific example/s, shall not be construed as limiting the meaning of the general wording preceding it and the *eiusdem generis* rule shall not be applied in the interpretation of that general wording or those specific example/s.
- 2.10 Where reference is made to clause and/or paragraph numbers it shall be a reference to clauses and/or paragraphs in this Policy unless it is expressly stated that the reference is made with regard to clause numbers in other documents, including but not limited to annexures or schedules to this Policy.

- 2.11 The use of any expression covering a process available under South African law such as a winding-up (within limitation *eiusdem generis*) shall, if any of the Parties is subject to the law of another jurisdiction, be construed as including any equivalent or analogous proceedings under the law of such defined jurisdiction.
- 2.12 The rule of interpretation of contracts that, in the event of ambiguity, the policy must be interpreted against the party responsible for the drafting of the policy does not apply.
- 2.13 The termination of this Policy does not affect those of its provisions which expressly provide that they will operate after termination, or which must continue to have effect after termination, or which must by implication continue to have effect after termination.

### **3. POLICY PURPOSE**

- 3.1. The Company and its Employees are the Responsible Parties for the processing of Personal Data obtained through its platforms, which without limitation includes, its websites. This Policy applies to all Personal Data processed by the Company and its Employees regardless of the location where the Personal Data is stored and regardless of the Data Subject.
- 3.2. The purpose of this Policy is to protect the Company from the compliance risks associated with processing of Personal Data, including breach of confidentiality, damage to reputation and failure to procure the necessary consent to use the Personal Data of the Data Subject.
- 3.3. This Policy entrenches the Company's commitment to the right to privacy and protection of Personal Data through compliance with POPIA and the GDPR and reasonable best industry practice, as well as a culture of privacy within the Company. The Company endeavors giving effect to the right of privacy and Personal Data through the implementation of the following practices:
  - 3.3.1. internal controls;
  - 3.3.2. practices which provide reasonable assurance that the rights of Data Subject are protected and balanced with the legitimate needs of the Company; and
  - 3.3.3. awareness training and guidance to individuals who process Personal Data.

#### **4. POLICY SCOPE AND APPLICATION**

- 4.1 The scope and application of this Policy shall, subject to POPIA and the GDPR, find application to the following persons:
- 4.1.1 All Employees who are employed by the Company whether on a permanent, part time and/or contract or temporary basis;
  - 4.1.2 All service providers who have entered into a contractual relationship with the Company for the supply of goods and/or services; and
  - 4.1.3 Any other relevant external parties engaged with the Company in their professional and/or personal capacity, which is not provided for above.
- 4.2 This Policy will be made available to all Associated Persons, upon the written request thereof by the aforementioned in electronic format and/or hard copy.
- 4.3 It is the responsibility of all Associated Persons as set out in this Policy, to familiarise themselves with the contents of this Policy as well as any accompanying schedule and/or annexure(s) attached hereto and as amended from time to time.

#### **5. POLICY PRINCIPLES**

- 5.1 Accountability
- 5.1.1 The Company and its Associated Persons will ensure POPIA, the GDPR and the provisions of this Policy are complied with through awareness training, building a culture of privacy, and encouraging desired behavior. The Company undertakes to pursue appropriate action against individuals who through their actions and/or omissions, be it intentional or negligent, fail to comply with this Policy.
- 5.2 Processing Limitation
- 5.2.1 Personal Data processed under the control of the Company and its Associated Persons will be processed in a fair, lawful, and limited manner, only with the consent of the Data Subject, and only for a specified purpose.
  - 5.2.2 Consent will be obtained prior to processing Personal Data from the Data Subject.
  - 5.2.3 The Data Subject must be informed that their Personal Data may be shared with



other entities by virtue of the nature of services provided by the Company.

### 5.3 Purpose Specification

5.3.1 The Company and its Associated Persons will only process Personal Data for a specific purpose and/or legitimate reasons of which the Data Subject must be informed of prior to processing.

### 5.4 Further Processing Limitation

5.4.1 The Company and its Associated Persons shall not process information for another purpose unless that purpose is directly relatable to the original specified purpose as communicated to the Data Subject. Should the processing of information for any other purposes be required, the Company and its Associated Persons shall procure the prior written consent from the Data Subject.

### 5.5 Open Communication

5.5.1 The Company and its Associated Persons shall take the necessary steps to ensure that Data Subjects are informed that their Personal Information is being collected and the purpose for which it is being processed.

### 5.6 Security Safeguards

5.6.1 The Company and its Associated Persons shall ensure that Personal Data is adequately protected by means of a secure filing system, with security measures to minimize risk of loss, unauthorized access, disclosure, interference, modification or destruction.

5.6.2 Security measures will be regularly reviewed and tested to prevent unauthorized access and to combat cyber-attacks on IT networks.

### 5.7 Transferring Personal Data

5.7.1 Personal Data will only be transferred where the prior consent of the Data Subject has been obtained, a legal obligation, in the performance of services by, or pursuit of a legitimate interest of the Company and its Associated Persons.

### 5.8 Data Minimization

5.8.1 The Company and its Associated Persons will only collect and process as much Personal Data as absolutely necessary and solely for the purposes specified by the Company.

5.9 Accuracy

5.9.1 The Company and its Associated Persons shall always take reasonable steps to ensure that the Personal Data that is stored by the Company is accurate and up to date.

5.10 Storage Limitation

5.10.1 All Personal Data processed by the Company and its Associated Persons will only be stored by the Company for as long as reasonably necessary for the specified purpose.

**6. WHEN IS DATA ALLOWED TO BE PROCESSED**

6.1 Data may only be processed by the Company and its Associated Persons in the following instances:

6.1.1 Where the Data Subject has given the Company and/or its Associated Persons specific, unambiguous consent to process the data;

6.1.2 Where the processing of the data is necessary to execute or to prepare to enter into a contract to which the Data Subject is a party;

6.1.3 Where the Company and/or its Associated Persons is required to process the Personal Data to comply with a legal obligation;

6.1.4 Where the Company and/or its Associated Persons is required to process the Personal Data to save an individual's life; and

6.1.5 Where the The Company and/or its Associated Persons has a legitimate interest to process the Personal Data.

**7. DATA BREACH**

7.1 The Company shall comply with all applicable laws regarding the notification of Data Subjects in the event of an unauthorized release of Personal Data and notification other unauthorized Personal Data and information disclosures.

7.2 The Company shall, within 72 hours of discovering any breach of the Company's security obligations or of any other event requiring notification under applicable law, notify the Data Subject, and any other individuals the law requires to be notified, of the breach or other events by telephone and/or by way of electronic mail.

## **8. TERM**

8.1 This Policy shall come into force and effect on the Commencement Date and shall continue thereafter for the Initial Term.

8.2 After the expiry of the Initial Term, this Policy shall be renewed by the Company.

8.3 Prior to the renewal of this Policy, the Company shall notify the Employees in writing within 3 (three) months prior to the expiration of the Initial Period, of its intention to extend this Policy, inclusive of the proposed terms of extension.

## **9. RULES IN TERMS OF THIS POLICY**

9.1 Associated Persons

9.1.1 All Associated Persons processing Personal Data on behalf of the Company will, during the course of their employment or performance of services, gain access to Personal Data under the control of the Company. These Associated Persons are required to treat Personal Data with the utmost care and confidentiality and are to respect the privacy of Data Subjects.

9.1.2 Associated Persons may not directly or indirectly disclose any part of Personal Data to the public, another unauthorized person or third party, either within or outside the organization, unless the information is already publicly known, or the disclosure is necessary to perform his/her duties or fulfil a lawful obligation.

9.1.3 Associated Persons must request clarification from the authorized management personnel if there is any uncertainty about any aspect related to the protection of Personal Data.

9.1.4 Associated Persons may only process information in the following circumstances:

9.1.4.1 the Data Subject has consented;

- 9.1.4.2 processing is necessary for the performance of duties or provision of services by the Responsible Party;
  - 9.1.4.3 a legal obligation on the Responsible Party;
  - 9.1.4.4 pursuit of a legitimate interest by the Responsible Party.
- 9.1.5 Associated Persons will under no circumstances:
- 9.1.5.1 process Personal Data which is not required to perform their work-related tasks or duties;
  - 9.1.5.2 save copies of Personal Data directly to their own private computers, laptops, tablets or mobile devices;
  - 9.1.5.3 share Personal Data informally or by means of unencrypted electronic communications (email, text message, etc.);
  - 9.1.5.4 transfer Personal Data without the express permission of the Data Protection Officer.
- 9.1.6 Associated Persons are responsible for:
- 9.1.6.1 taking sensible precautions to keep all Personal Data they come into contact with secure;
  - 9.1.6.2 keeping areas where Personal Data may be found organized and to a minimum, with all confidential information out of view from unauthorized persons at all times;
  - 9.1.6.3 ensuring Personal Data is encrypted prior to transmitting electronically;
  - 9.1.6.4 making sure all computers, laptops, tablets, mobile devices, flash drives and any other device containing Personal Data is password protected and never left unattended where it may be accessed by an unauthorized person. Passwords must be changed regularly and never shared with unauthorized persons or stored as plain-text;

9.1.6.5 switching off devices or locking the screen when not in use (external drives, CDs, DVDs and other removable storage devices must be locked away when not in use);

9.1.6.6 undergoing and taking proper note of awareness training provided to them;

9.1.6.7 ensuring Personal Data is never discussed in public areas or with unauthorized individuals.

9.1.6.8 Should a person suspect or be aware of any security breach or breach of this Policy, they must immediately report it to the Data Protection Officer.

9.1.7 Disclosing of Confidential Information

9.1.7.1 Confidential Information will not under any circumstances be disclosed to any third party by any Associated Persons without prior written authority from the Data Protection Officer.

9.1.7.2 Any requests directed to any Associated Persons for information that is considered to be Personal Data should be referred to the Data Protection Officer, who will, in consultation with Mr Flippie Groenewald, review and prepare a response in line with the applicable laws.

## **10. DATA SUBJECT ACCESS REQUESTS**

10.1 All Data Subjects are entitled to request information from the Company pertaining to the Data Subject's Personal Data that is held by the Company.

10.2 All requests for information should be made in writing by the Data Subject to the Company. The Company will furnish the Data Subject with the requested information within 14 (fourteen) days from the date of receipt of the written request by the Company.

10.3 Prior to furnishing the Data Subject with the requested information, the Company will first have to verify the identity of the Data Subject.

## **11. ENQUIRY PROTOCOL AND GUIDELINES**

11.1 All Associated Persons are prohibited from commenting and/or making any public statement in respect of the Personal Data/information unless prior written approval (which may or may not include limitations) have been obtained Data Protection Officer.

11.2 All Associated Persons shall notify Data Protection Officer in writing should a third party contact the Associated Person regarding any Personal Data/information related matter.

11.2.1 The written notification contained in 11.2 above, shall, without limitation, include the following information:

11.2.1.1 The full names and identity number of the third party;

11.2.1.2 The contact details of the third party; and

11.2.1.3 The nature and purpose of the third party contacting the Associated Person.

11.2.2 Upon receipt of the notification contained in 11.2 above, the Data Protection Officer shall as soon as reasonably possible formulate a written review and recommendation which shall be submitted to Flippie Groenewald for consideration and approval.

11.2.3 Flippie Groenewald shall as soon as reasonably communicate his decision (along with any comments regarding the implementation of the decision, where applicable) to Data Protection Officer.

11.2.4 The Data Protection Officer shall give effect and implement the findings of Flippie Groenewald an efficient manner.

11.2.5 For sake of clarity, an Associated Person shall under no circumstances disseminate any Personal Data/information, unless obtaining the prior written approval from the Data Protection Officer and Flippie Groenewald.

## **12. BREACH OF THIS POLICY**

### **12.1 By Employee(s)**

12.1.1 Any breach of this Policy by an Employee shall result in disciplinary action being taken against the Employee in terms of the disciplinary procedures of the Company.

12.1.2 In the event that an Employee fails to comply with this Policy, the Company may at their sole and absolute discretion:

12.1.2.1 institute disciplinary action against that Employee, which may result, without limitation, result in:

12.1.2.1.1 the Employee being furnished with written warning (first and/or final); and/or

12.1.2.1.2 the dismissal of Employee.

12.1.2.2 Report the matter to the relevant civil or criminal bodies for further action in terms of the laws of South Africa.

12.1.3 An Employee shall within twenty-four (24) hours of termination of employment, remove all references to the Company from their personal Social Media platforms and/or accounts.

**12.2 By any Person(s)**

12.2.1 Should any Person commit a Breach of any provision of this Policy and, if such Breach is capable of being remedied, fails to remedy the Breach within 5 (five) business days after the delivery to the Person of written notice by the Company requiring that the Breach be remedied, the Company shall, in addition and without prejudice to any other rights which it may have in terms of this Policy or in law, terminate any contractual relationship that subsists with the Person at the relevant time and claim damages, alternatively claim specific performance and/or any damages suffered.

12.2.2 Should the Company instruct attorneys to take any action in terms hereof, then the Person agrees and undertakes to pay all costs incurred by the Company on an attorney and own client scale, which may arise as a result of the breach of any term in this Policy.

**13. REVIEW, MONITORING AND EVALUATION OF THE POLICY**

**13.1 Monitoring**

13.1.1 The Data Protection Officer shall be responsible for monitoring the application of this Policy, which shall without limitation include the following:

13.1.1.1 Monitoring all internal and external operating systems utilised by the Company's Employees which relates directly or indirectly to the Company;

13.1.1.2 Deal with any breach situations and shall mitigate any reputational risk;

13.1.1.3 Support and advise Flippie Groenewald on appropriate actions; and

13.1.1.4 Monitor and analyse the Policy implementation to identify trends and issues that warrant the attention of the Company.

### 13.2 **Evaluation**

13.2.1 An evaluation report shall, at the sole and absolute discretion of the Company be prepared annually and circulated to all Employees of the Company.

13.2.2 The dissemination of the evaluation report serves to encourage comment and participation of Employees to facilitate improving the Policy for all stakeholders concerned.

### 13.3 **Review**

13.3.1 This Policy shall, at the sole and absolute discretion of the Company be reviewed every 2 (two) years or as and when is required by Flippie Groenewald.

13.3.2 Any amendments may, upon the written request of an Employee and/or other Persons be made available. In this regard, it is the responsibility of all Associated Persons as defined in this Policy to keep updated with any amendments to the Policy.