Dotport Capital (Pty) Ltd
(Reg no 1997/006386/07)
&
Dotport (Pty) Ltd
(Reg no 1998/014064/07)
&
Dotvest (Pty) Ltd
(Reg no 1996/009579/07)

Protection of Personal Information Policy

in terms of the

Protection of Personal Information Act

1. Definitions

a. In this document "we" and "us" refer to Dotport (Pty) Ltd, Dotport Capital (Pty) Ltd and/or Dotvest (Pty) Ltd as entities in combination or individually and/or to its management and/or employees. "We" and "us" refer to as the "Responsible Party"
b. "Data Subject" means the person to whom personal information relates.
c. "Personal information" means information relating to an identifiable, living, natural, and where it is applicable, an identifiable, existing juristic person.
d. "Processing" involves anything that is done with personal information. This includes collection, use storage, dissemination, modification or destruction of personal information.
e. "Responsible Party" means a public or private body or any other person which, alone or in conjunction with other, determines the purpose of and means for processing personal information.

2. Purpose of the Act

The purpose of this Act is to:-

1. Give effect to right to privacy, by safeguarding personal information when processed, subject to limitations that are aimed at-
   a. Balancing the right to privacy against other rights, particularly the right to access to information.
   b. Protecting important interests, including the free flow of information within the borders and across international borders.
2. Regulate the manner in which personal information may be processed, by establishing conditions that prescribe the minimum requirements for the lawful processing of personal information.
3. Provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act.
4. Establish voluntary and compulsory measures to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

3. Lawful processing of personal information

1. The conditions for the lawful processing of personal information by or for a responsible are the following:

a. Accountability
b. Processing limitation
c. Purpose specification
d. Further processing limitation
e. Information Quality
f. Openness
g. Security safeguards
h. Data subject participation

4. Rights of Data subjects

1. A data subject has the right to have his information processed in accordance with the conditions for the lawful processing of personal information, including the right
   a. To be notified that personal information about hom is being collected or his information has been accessed or acquired by an unauthorised person. (Section 18 & 22)
   b. To establish whether a responsible party holds personal information of him to request access to his personal information. (Section 23)
   c. To request the correction, destruction or deletion of his personal information. (Section 24)
   d. To object relating to his particular situation to the processing of his personal information (Section 11(3)(a))
   e. To object to the processing of his personal information at any time for purposes of direct marketing. (Section 11(3)(b) & 69)
   f. Not to have his personal information processed for puposes of direct marketing by means of unsolicited electronic communications. (Section 69(1))
   g. Not to be subject to a decision which is based solely on the basis of the automated processing of his personal information intended to provide a profile of him. (Section 71)

h. To submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information. (Section 74)
i. To institute civil proceedings regarding the alleged interference with the protection of his personal information. (Section 99)

5. Responsible party to ensure conditions for lawful processing

1. The responsible party must ensure that the measures that give effect to such conditions in terms of lawful processing, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

6. Lawfulness of processing

1. Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

7. Minimality

1. Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

8. SECTION 11 Consent, justification and objection

1. Personal information may only be processed if
   a. The data subject consents to the processing.
   b. Processing is necessary to carry out actions for the conclusion of a contract to which the data subject is party.
   c. Processing complies with an obligation imposed by law on the responsible party.
   d. Processing protects a legitimate interest of the data subject.
   e. Processing is necessary for the proper performance of a public law duty by a public body.
   f. Processing is necessary for pursuing the legitimate interest of the responsible party.
2. The responsible party bears the burden of proof for the data subjects consent.
3. The data subject may withdraw his consent at any time.
4. A data subject may object, at any time, to the processing of personal information
   a. On reasonable grounds relating to his particular situation, unless legislation provides for such processing.
   b. For purposes of direct marketing.
5. If a data subject has objected to the processing of personal information the responsible party may longer process the personal information.

9. Collection directly from data subject

1. Personal Information must be collected directly from the data subject, except for the following:
   a. The information is from a public record or has been deliberately been made by the data subject.
   b. The data subject or a competent person representing a child, has consented to the collection of information from another source.
   c. Collection of the information from another source would not prejudice a legitimate interest of the data subject.
   d. Collection of the information from another source is necessary :
      -To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences.
      -To comply by an obligation imposed by law concerning collection of revenue for SARS.
      -For the conduct of proceedings in any court that has commenced or are reasonably contemplated.
      -In the interest of national security.
      -To maintain the legitimate interest of the responsible party to whom the information is supplied.
   e. Compliance would prejudice a lawful purpose of the collection.
   f. Compliance is not reasonably practicable in the circumstances of the particular case.

10. Collection for specific purpose

1. Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.
2. Steps must be taken in accordance with Section 18(1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of section 184) are applicable.

11. Retention and restriction of records

1. Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected.
2. In term of FAIS and the FIC Act records must be retained for a period of 5 years after the relationship has ended. Note that if there was not relationship started with a new client, in other word just a presentation, the information must not be retained, unless the parties agree to the retention of the information.
3. Records of personal information must be destroyed or deleted as soon as reasonably practicable after the responsible is no longer authorised to retain the record.
4. The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

12. Further processing to be compatible with purpose of collection

1. Further processing of personal information must be in accordance or compatible with the purpose for which it was collected.
2. Personal information can be used for follow-ups in terms of the six steps of financial planning. No other reason.

13. Quality of Information

1. Practical steps must be taken to ensure that personal information is complete, accurate, not misleading and updated where necessary.
2. The responsible party must have regard to the purpose for which the information was collected.
3. Practically information must be verified, eg copy of ID, policy information from companies, etc.

14. Documentation

1. Documentation must be maintained of all processing operations.

15. Notification to data subject when collecting personal information

1. If personal information is collected, we must take reasonable practicable steps te ensure that the data subject is aware of:
   a. The information being collected and where the information is not collected from the data subject, the source from which it is collected.
   b. The name and address of the responsible party.
   c. The purpose for which the information is being collected.
   d. Whether or not the supply of the information by the data subject is voluntary or mandatory.
   e. The consequences of failure to provide the information.
   f. Any particular law authorizing or requiring the collection of the information.
   g. The fact that, where applicable, we intent to transfer the information to a third country or international organization and the level of protection afforded to the information by that party.
   h. Any further information such as the
      -The recipient or category of recipients.
      -Nature or category of information.
      -Existence of the right of access to and the right to rectify the information collected.
      -Existence of the right to object to the processing of personal information as referred to in section 11(3).
      -Right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator.
2. The above steps must be taken:
   a. If the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to above.

b. In any case, before the information is collected or as soon as reasonably practicable after it has been collected.

3. A responsible party that has previously taken the steps referred to above, complies with subsection 1 in relation to the subsequent collection from the data subject of the same information of the same kind if the purpose of collection of the information remains the same.
4. It is not necessary for the responsible party to comply with subsection 1 if:
   a. The data subject or a competent person where the data subject is a child has provided consent for the non-compliance.
   b. Non-compliance would not prejudice the legitimate interests of the data subject.
   c. Non-compliance is necessary in criminal investigations, SARS, proceedings of a court or in the interest of national security.
   d. Compliance would prejudice a lawful purpose of the collection.
   e. Compliance is not reasonable practicable in the circumstances of a particular case.
   f. The information will:
      -Not be used in a form in which the data subject may be identified, or
      -Be used for historical, statistical or research purposes.

16. Security measures on integrity and confidentiality of personal information

1. The integrity and confidentiality of personal information in possession must be secured and appropriate, reasonable technical and organizational measures to prevent:
   - Loss, damage or unauthorised destruction of personal information.
   - Unlawful access to or processing of personal information.
2. The following must be implemented to address the above:
   a. Identify all foreseeable internal and external risks.
   b. Establish and maintain appropriate safeguards against the risks identified.
   c. Regularly verify that the safeguards are effectively implemented.
   d. Regularly update safeguards.

17. Information processed by operator of person acting under authority

1. Anyone processing personal information on half of a responsible party must:
   a. Process the information only with the knowledge or authorisation of the responsible party.
   b. Treat personal information as confidential and must not disclose it.

18. Security measures regarding information processed by operator

1. A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator establishes and maintains the security measures refer to in section 19.
2. The operator must notify the responsible party 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.

19. Notification of security Compromises

1. When personal information has been access or acquired by any unauthorised person, the responsible party must notify:
   -The Regulator
   -The data subject, unless the data of the data subject cannot be established.
2. The notification must be as soon as possible.
3. The notification to the data subject must be in writing and communication in at least one of the following ways:
   -Mailed by post
   -Email
   -Placed on a prominent position on the website of the responsible party.
   -Published in the news media
   -As may be directed by the Regulator.
4. The notification must provide the following information:
   a. A description of the possible consequences of the security compromise.
   b. A description of the measures that the responsible party intends to take or has taken to address the security compromise.

c. A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise.
d. The identity of the unauthorised person if known.

20. Access to personal information

1. A data subject, having provided adequate proof of identity, has the right to:
   a. Request us to confirm whether or not we hold personal information about the data subject.
   b. Request the record or a description of personal information about the data subject held by us, including information about the identity of all third parties who have or have had access to the information.
2. The data subject must be made aware that it has the right to request correction of information.
3. We may of must refuse to disclose information in terms of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the POPIA.
4. The provisions of section 30 & 61 of the POPIA are applicable in respect of access to health or other records.

21. Correction of personal information

1. A data subject my request us to:
   a. Correct/delete personal information that is inaccurate, excessive, out of date, incomplete, misleading or obtained unlawfully, or
   b. Destroy/delete a record of personal information that we are not authorised to retain in terms of section 14.
2. On receipt of the above request, we must:
   a. Correct the information
   b. Destroy/delete the record
   c. Provide the data subject with credible evidence in support of the information.
   d. Where agreement cannot be reached between us and the data subject, and if the data subject so request, take such steps as are reasonable in circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.
3. If we have taken steps under subsection 2 that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, we must if reasonably practically, inform everybody to whom the personal information has been disclosed of those steps.
4. We must notify a data subject, who has made a request in terms of subsection 1, of the action taken as a result of the request.

22. Manner of access

1. The provisions of section 18 & 53 of POPIA apply to requests made in terms of section 23 of this Act.

23. Prohibition on processing of special personal information

1. We may, subject to Section 27, not process personal information concerning:
   a. 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.
   b. The criminal behaviour of a data subject.

24. General authorisation concerning special personal information

1. The prohibition on processing personal information, as referred to in section 26, does not apply if the:
   a. Processing is carried out with the consent of a data subject.
   b. Processing is required for the establishment, exercise or defense of a right or obligation by law.
   c. Refer to Section 27 1.c-d and 2 & 3.

25. SECTION 32 OF THE ACT Authorisation concerning data subject's health or sex life.

1. The prohibition on processing personal information concerning a data subject's health or sex life, as referred to in section 26, does not apply to the processing by

a. See Section 32 of the Act
b. Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for
-Assessing the risk to be insured
-Performance of the insurance or medical scheme agreement.
-The enforcement of any contractual rights and obligations.
c. See Section 32 of the Act.
d. See Section 32 of the Act.
e. See Section 32 of the Act.
f. Administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for:
-The implementation of the pension, etc.
-The reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

2. The information may only be processed subject to confidentiality.

26. General authorisation concerning personal information of children

1. Personal information of a child can be processed if it is:
   a. Carried out with the prior consent of a competent person.
   b. Necessary for the establishment, exercise or defence of a right or obligation by law.
2. We must establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

27. Duties and responsibilities of Information Officer

1. An information officer's responsibility include:
   a. The encouragement of compliance with the conditions for the lawful processing of personal information.
   b. Dealing with the requests made pursuant to this Act.
   c. Working with the Regulator in relation to investigations conducted pursuant to Chapter 6.
   d. Otherwise ensuring compliance with the compliance of this Act.
2. Officers may take up their duties in terms of this Act only after the responsible party has registered with the Regulator.

28. Designation and delegation of deputy information officers

1. We must make provision, in the manner described in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of:
   1. Such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in Section 55.
   2. Any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of us.

29. Direct marketing by means of unsolicited electronic communication

1. The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or email is prohibited unless the data subject:
   a. Has given consent to the processing, or
   b. Is subject to subsection 3, a customer of the responsible party.
2. A responsible party may approach a data subject only once to request the consent of that data subject:
   -Whose consent is required in terms of subsection 1a; and
   -Who has not previously withheld such consent.
   -The data subject consent must be requested in the prescribed manner and form.
3. A responsible party may only process personal information of a data subject who is a customer of the responsible party in terms of subsection 1b:
   a. If the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service.
   b. For the purpose of direct marketing of the responsible party's own similar products or services.
   c. If the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details:

-At the time when the information was collected
-On the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

4. Any communication for the purpose of direct marketing must contain:
    a. Details of the identity of the sender or the person on whose behalf the communication has been send. And
    b. An address or other contact details to which the recipient may send a request that such communication cease.
5. Automatic calling machine means a machine that is able to do automated calls without human intervention.

30. Transfers of personal information outside SA

1. We may not transfer personal information about a data subject to a third party who is in a foreign country unless:
    a. The third party is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection.
    b. The data subject consent to the transfer.
    c. The necessary for the performance of a contract between the data subject and us, or for the implementation of pre-contractual measures taken in response to the data subject's request.
    d. The transfer is necessary for a contract concluded in the interest of the data subject between the data subject and us. Or
    e. The transfer is for the benefit of the data subject, and
    -It is not reasonable practicable to obtain the consent of the data subject to that transfer; and
    -If it were reasonable practicable to obtain consent, the data subject would be likely to give it.

31. Complaints

1. Should you believe that we have utilised your personal information contrary to applicable laws, you undertake to first attempt to resolve any concerns with us.
2. If you are not satisfied with such process, you have the right to lodge a complaint with the Information Regulator at complaints.IR@justice.gov.za and/or www.justice.gov.za/inforeg/.

32. Contact us

1. We have appointed Information Officers who are responsible for ensuring that we are compliant with relevant data protection laws. Please feel free to contact us info@dotport.co.za should you have any questions.