


ANNEXURE A

	DENEL SOC LTD COMPANY POLICY	NUMBER
SUBJECT: PRIVACY POLICY AND DATA PROTECTION POLICY		EFFECTIVE DATE 1 JULY 2021
<ol style="list-style-type: none">1. APPLICATION OF THE POLICY2. PRIVACY AND DATA PROTECTION POLICY STATEMENT3. BACKGROUND4. PURPOSE5. DEFINITIONS6. CONDITIONS FOR PROCESSING PERSONAL INFORMATION<ol style="list-style-type: none">6.1 Accountability6.2 Process limitation6.3 Purpose Specification6.4 Further processing of personal information6.5 Information quality6.6 Openness6.7 Security safeguards6.8 Data subject participation6.9 Processing of Special Personal Information7. NOTIFICATION OF COMPROMISE OF PERSONAL INFORMATION8. POLICY ADMINISTRATION9. REVISION HISTORY10. ANNEXURES		
COMPILED BY: GROUP RISK & COMPLIANCE MANAGER	APPROVED BY THE DENEL BOARD	SIGNATURE GROUP CHIEF EXECUTIVE OFFICER



PRIVACY POLICY AND DATA PROTECTION POLICY

1. APPLICATION OF THE POLICY

This policy applies to information relating to identifiable individuals, in terms of the Protection of Personal Information Act, 2013 (hereinafter POPI Act) applies to Denel (SOC) Limited and its subsidiaries as enumerated below:

1.1. Denel SOC Limited

Physical:

*Irene Campus
Nellmapius Drive
IRENE*

Postal Address:

*P O Box 8322
CENTURION
0046*

Switchboard Number: 012 671 2700

DENIPROP

Physical:

*Irene Campus
Nellmapius Drive
IRENE*

Postal Address:

*PO Box 15504
IMPALA PARK
1472*

Switchboard Number: 012 671 2700

1.2. Denel Aeronautics

Physical:

*Denel Kempton Park Campus
Atlas Road
BONAERO PARK
1619*

Postal Address:

*P O Box 7246
BONAERO PARK
1622*

Switchboard Number: 011 927 2084



- 1.3. Denel Dynamics
Physical:
*Irene Campus
Nellmapius Drive
IRENE*
- Postal Address:**
*P O Box 7412
CENTURION
0046*
- Switchboard Number: 012 671 2700*
- 1.4. Denel Land Systems
Physical:
*Lyttelton Campus
368 Selbourne Avenue
LYTTELTON*
- Postal Address:**
*P O Box 7710
PRETORIA
0001*
- Switchboard Number: 012 620-9111*
- 1.5. Denel OTR
Physical:
*Arniston Road
BREDASDORP*
- Postal Address:**
*Private Bag X12
BREDASDORP
7280*
- Switchboard Number: 028 445 2000*
- 1.6. PMP
Physical:
*1 Ruth First Street
LOTUS GARDENS
0008*
- Postal Address:**
*Private Bag X334
PRETORIA
0001*



**DENEL SOC LTD
COMPANY POLICY**

Switchboard Number: 012-318 1911

1.7. Denel Aerostructures (SOC) Ltd

Physical:

*Denel Kempton Park Campus
Atlas Road
BONAERO PARK
1619*

Postal Address:

*P O Box 7246
BONAERO PARK
1622*

Switchboard Number: 011 927 2084

1.8. Denel Vehicle Systems

Physical:

*12 Barnsley Road
BENONI
1501*

Postal Address:

*Private Bag X049
BENONI
1500*

Switchboard Number: 011 747 3300

1.9. Densecure.

Physical:

*Irene Campus
Nellmapius Drive
IRENE*

Postal Address:

*P O Box 8322
CENTURION
0046*

Switchboard Number: 012 671 2700

1.10. **CHIEF INFORMATION OFFICER**

Denel SOC Limited

Physical:

Irene Campus



DENEL SOC LTD COMPANY POLICY

*Nellmapius Drive
IRENE*

Postal Address:

*P O Box 8322
CENTURION
0046*

Switchboard Number: 012 671 2700

2. PRIVACY AND DATA PROTECTION POLICY STATEMENT

In conducting business Denel may collect information including for hiring, commercial agreements, procurement and for payment purposes as well as for granting access to its premises as part of conducting its legitimate business. Some of the information that Denel collects falls within the definition of Personal Information which is subject to the provisions of the Protection of Personal Information Act 4 of 2013. The protection of Personal Information and complying with applicable laws and regulations is an important aspect of good governance obligation. To this end Denel undertakes to:

- 2.1 Comply with the provisions of the Protection of Personal Information Act 4 of 2013 and other relevant laws and regulations regarding the processing of personal information including;
 - 2.1.1 Making the Data subject aware of the purpose for collecting their Personal Information;
 - 2.1.2 Explicitly defining and outlining reasons to the data subject for processing Personal Information for further purposes;
 - 2.1.3 Taking reasonable steps to ensure that information is complete, accurate, not misleading and, where necessary, updated;
 - 2.1.4 Where applicable, making the Data subject aware regarding the following:
 - 2.1.4.1 Whether the supply of information by the data subject is voluntary or mandatory;
 - 2.1.4.2 The consequences of failing to provide information
 - 2.1.4.3 The legislation requiring the collection of information
 - 2.1.4.4 Where information is to be transferred to another country, information relating to the laws that will protect the information.
- 2.2 Only use personal information processed for the purpose and duration it was required;
- 2.3 Obtain requisite consent prior to processing any of the Personal Information for purposes other than the purpose for which the information was collected;
- 2.4 Obtain authorisation/consent required for the processing and transfer of Special Personal Information;
- 2.5 Lawfully process all personal information with due regard to the conditions of; Accountability, Process limitation, Purpose Specification, Further processing of Personal Information, Information quality, Openness, Security safeguards and Data subject



participation set out in the Protection of Personal Information Act 4 of 2013

- 2.6 Safeguard Personal Information once it is in its possession to prevent unlawful processing by ensuring that:
- (i) Access to Personal Information is controlled to prevent data leaks, loss, unlawful processing, destruction and/or damage;
 - (ii) Employees, Contractors, Service Providers and Board Members with access to Personal Information comply with the requirements of the Protection of Personal Information Act 4 of 2013;
 - (iii) Measures are taken for all Contractors and Service Providers to ensure the protection of Personal Information.
- 2.7 Implement digital and physical measures to secure Personal Information it processes.
- 2.8 Ensure that all staff who have access to Personal Information are duly trained regarding Personal Information and their responsibilities in this regard.

3. BACKGROUND

The Protection of Personal Information Act 4 of 2013 [POPIA] gives effect to the right to privacy set out in section 14. The Act balances the right to privacy against other rights, particularly, the right of access to information. The Act regulates the manner in which Personal Information may be processed by public bodies (like Denel SOC Ltd) and private bodies.

Denel is obliged by law to put in place appropriate internal controls to ensure the processing and safeguarding of personal information within its control is in compliance with the POPIA.

4. PURPOSE

The purpose of this policy is to ensure that the processing of personal information is processed and safeguarded in compliance with the POPIA and any other relevant regulations.

5. DEFINITIONS

Data Subject: means a natural or juristic person to whom the personal information relates;

Responsible Party: means 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;

Processing: means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

- (i) the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- (ii) dissemination by means of transmission, distribution or making available in any other form; or
- (iii) merging, linking, as well as restriction, degradation, erasure or destruction of information



Record: means any writing on any material, labels, books, maps, plans, graphs, drawings and photographs, films, negatives, tapes or other devices where visual images are stored.

Information Officer: means, in relation to, a—

- (a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or
- (b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

Regulator: means the Information Regulator established in terms of section 39 of the POPIA;

Functional Head: means the executive whose function involves processing Personal Information

Operator: means a person who processes Personal Information on behalf of the Responsible Party in terms of contract between them without coming under direct authority of the RP

Special Personal Information: means personal information as referred to in section 26 of the POPIA namely:

1. the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
2. the criminal behaviour of a data subject to the extent that such information relates to—
 1. the alleged commission by a data subject of any offence; or
 2. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

Personal Information: means “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- a) 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;
- b) information relating to the education or the medical, financial, criminal or employment history of the person;
- c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
- d) the biometric information of the person;
- e) the personal opinions, views or preferences of the person;
- f) 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;
- g) the views or opinions of another individual about the person; and
- h) 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.”

6. CONDITIONS FOR PROCESSING PERSONAL INFORMATION

All Personal Information will be processed in compliance with the following conditions.

6.1 Accountability



DENEL SOC LTD COMPANY POLICY

- 6.1.1 Collecting as minimum of Personal Information as possible securely and as is adequate to fulfil its purpose as to not compromise the privacy of the Data subject.
- 6.1.2 Determining the purpose and means for processing Personal Information, in full compliance with the conditions set out in the Act 4 of 2013.
- 6.1.3 Ensuring that Operators as part of their written contracts under the supervision of the relevant Functional Heads:
 - 6.1.3.1 Process information only with the knowledge of Denel;
 - 6.1.3.2 Treat Personal Information confidentially;
 - 6.1.3.3 Secure Personal Information; and
 - 6.1.3.4 Inform the Functional Head and the Information Officer of any breach immediately
- 6.1.4 Denel shall appoint a and register with the Regulator a Information Officer who is duly authorised by Denel to work with the Regulator, deal with requests from data subjects relating to their Personal Information and ensure full compliance with the POPIA

6.2 Process limitation

- 6.2.1 Limiting the processing of Personal Information to protecting or pursuing legitimate interests or for the proper performance of a public law duty, to conclude or perform a contract to which the Data Subject is party and to fulfill obligations imposed by law.
- 6.2.2 Limiting the processing of personal information to lawful processing and must not infringe the privacy of the Data Subject.
- 6.2.3 The purpose of processing must be adequate, relevant and not excessive and with the consent of the Data Subject.
- 6.2.4 Obtaining Personal Information directly from the Data Subject except where the information is derived from a public record or the Data Subject has consented to the use of another source or has made the information public.
- 6.2.5 In order to achieve the above the relevant Functional Head shall:
 - 6.2.5.1 Set the requirements for minimum information to prevent excessive information that may infringe the Privacy Rights of the Data Subject
 - 6.2.5.2 Implement processes for lawful processing based on minimum information, consent, justification and object of processing and collecting information directly from data subject as may be appropriate.
 - 6.2.5.3 Implement processes to ensure the information provided is relevant and adequate.

6.3 Purpose Specification

- 6.3.1 The purpose of Personal Information collected must be specific, explicitly defined and lawful and related to a function or activity of Denel and the Data Subject must be informed of the purpose of collecting Personal Information.
- 6.3.2 Personal Information may be kept for a specific duration limited to the purpose for which



the Personal Information was required, as agreed between parties, consent of the Data Subject or longer as otherwise prescribed by statutory provisions.

- 6.3.3 Personal Information must be destroyed in a manner that prevents its reconstruction in an intelligible form when Denel is no longer authorised to retain such Personal Information.
- 6.3.4 In order to achieve the above, the relevant Functional Heads shall ensure that:
 - 6.3.4.1 The purpose for Personal Information is specific, explicitly defined and relevant to the context and the function for which it is required;
 - 6.3.4.2 The Data Subject is aware of the purpose for collection of Personal Information
 - 6.3.4.3 Personal Information is retained only for as long as necessary to achieve the purpose for which Personal Information was collected, or longer unless authorised by law, or for lawful purposes of Denel, contract between parties or consent of the Data Subject.
 - 6.3.4.4 Personal Information is destroyed in a manner that prevents its reconstruction in an intelligible form when Denel is no longer authorised to retain such Personal Information.

6.4 Further processing of personal information

- 6.4.1 Personal information may be used for further processing if such is compatible with or in accordance with the purpose for which it was collected in the first place.
- 6.4.2 The test for compatibility must be applied to decide further processing of Personal Information.
- 6.4.5 In order to achieve the above, the relevant Functional Heads are responsible for implementing processes that ensure that:
 - 6.4.5.1 Where further processing of personal information is done it is compatible with or in accordance with the purpose for which Personal Information was collected in the first place in compliance with the Test for Compatibility.

6.5 Information quality

- 6.5.1 Reasonable practical steps are to be taken to ensure that Personal Information is complete, accurate, not misleading and updated where necessary.
- 6.5.2 Special care must be taken where information is collected from a source other than the Data Subject.
- 6.5.3 The relevant Functional Heads are responsible for implementing processes that ensure:
 - 6.5.3.1 Personal Information, complete, accurate and not misleading
 - 6.5.3.2 Personal Information is updated/corrected as may be necessary
 - 6.5.3.3 Data subjects have access to update their Personal Information

6.6 Openness

- 6.6.1 Reasonable steps are to be taken to make the Data Subject aware of the information collected and the source of the information, the name and address of the entity collecting the information, the purpose for which it is collected, whether the Data Subject is obliged to supply the information and what law if any prescribes the disclosure of the information to the Responsible Party.
- 6.6.2 The Data Subject must be informed exactly what information will be processed, to whom and the Data Subject's right to access and update the information collected or to complain to the Regulator when the Responsible Party intends to transfer the information across the border
- 6.6.3 The relevant Functional Heads are responsible for:
 - 6.6.3.1 Maintaining the documentation of all processing operations under their responsibility



6.6.3.2 Ensuring that Personal Information is processed only if the Data Subject is aware that the information is being collected, Name and address of Responsible Party, Purpose of collection, whether disclosure is voluntary or mandatory, Consequences of failure to provide information, laws authorizing collection of information and that Personal Information will be transferred to across the border.

6.6.3.3 The Data Subject is to be informed of the protection that the information will have in the foreign country or with the international organisation when transferred cross border .

6.7 Security safeguards

6.7.1 Measures are to be taken to secure Personal Information including its integrity and confidentiality from internal and external exposures using generally accepted information security practices and procedures.

6.7.2 The relevant Functional Heads are responsible for implementing:

6.7.2.1 Digital, physical and administrative security measures to prevent loss of or damage to or unauthorised destruction, unlawful access to or processing of Personal Information.

6.7.2.2 Process in terms of which, where there are reasonable grounds to belief that the personal information has been accessed or acquired by any unauthorised person the Regulator and the Data Subject are notified in a prescribed manner and form.

6.8 Data subject participation

6.8.1 A Data subject may with proof of identity, requests the Responsible Party to confirm whether it is holding its Personal Information, free of charge.

6.8.2 The Data Subject may request a description of Personal Information or record thereof within a reasonable time and at a reasonable fee.

6.8.3 The Data Subject is entitled to know which third parties have or had access to the personal information.

6.8.4 A Data Subject has a right to request correction or delete the Personal Information.

6.8.5 Denel must inform the Data subject what action has been taken pursuant to the request for a correction.

6.8.6 Denel must correct or delete the information subject to a request for correction or provide proof of the correctness of the information and attach a note to the record reflecting both the request and the response.

6.8.7 An employee has a right in the prescribed form to request the records or a description of the personal information that Denel holds. An employee is also entitled to know which third parties have or had access to the personal information.

6.8.8 The Manner for access to Personal Information is as provided for in Promotion of Access to Information Act.

6.8.9 Upon request Denel must furnish the records or information unless Denel may rely on one of the grounds in the Promotion of Access to Information Act to refuse the record or information.

6.8.10 The relevant Functional Heads are responsible to ensure that the above requirements are infused in the relevant management processes.

6.9 Processing of Special Personal Information

6.9.1 Special Personal Information may only be processed with the consent of the Data Subject unless processing is necessary for the establishment, exercise or defence of a right or obligation in law or the Data Subject has already made the information available publicly.



- 6.9.2 The regulator may also authorise processing of special personal information if it is in the public interest and subject to appropriate safeguards and the Responsible Party may also rely on any of the listed exceptions.
- 6.9.3 The Responsible Party may without consent of the Data Subject:
 - 6.9.3.1 Use Personal Information concerning race or ethnic origin to comply with legislation.
 - 6.9.3.2 Process Personal Information concerning the health of an employee if it is necessary for the administration of retirement funds and medical schemes or to reintegrate or support employees entitled to incapacity or ill health benefits.
 - 6.9.3.3 Process special personal information to comply with collective bargaining obligations.

7. NOTIFICATION OF COMPROMISE OF PERSONAL INFORMATION

- 7.2.5 When there are reasonable grounds to believe security compromise of Personal Information, the Responsible Party must notify the Regulator and Data Subject (unless DS cannot be identified) as soon as possible after discovery of compromise.
- 7.2.6 Notification to the Regulator must:
 - 7.2.6.1 Be in writing and sufficient provide sufficient information to allow DS to take preventative measures;
 - 7.2.6.2 Include possible consequences
 - 7.2.6.3 Explain measures that the Responsible Party intends to take
 - 7.2.6.4 Recommended measures to be taken by Data Subject
 - 7.2.6.5 Give the identity of unauthorized persons

8. POLICY ADMINISTRATION

The policy shall be reviewed when the business process, or new standards and even legislation warrant or to address deficiencies found identified during an audit.

9. REVISION HISTORY

Date	Version	Comments
1 July 2021	001	



ANNEXURE A

6. DUTIES OF THE INFORMATION OFFICER

- 6.1 Section 55(1) of POPIA sets out the duties and responsibilities of an Information Officer which include the following: -
- 6.1.1 the encouragement of compliance by the body with the conditions for the lawful processing of personal information. For example-
- 6.1.1.1 an Information Officer may develop a policy on how employees should implement the eight (8) conditions for the lawful processing of personal information or consider issuing a circular in the case of provincial and national departments;
- 6.1.2 dealing with requests made to the body pursuant to POPIA. For example-
- 6.1.2.1 an Information Officer of a body will be expected to render such reasonable assistance, free of charge, as is necessary to enable the requester or data subject to comply with the prescribed process for submitting a request in terms of section 18 of PAIA² and section 24 of POPIA³. If a requester or data subject has made any request that does not comply with the requirements of PAIA or POPIA, the Information Officer concerned may not refuse the request because of that non-compliance, unless the Information Officer has
- notified the data subject or requester of his/her intention to refuse the request and stated in the notice, the reasons for the contemplated refusal, as well his/her availability to assist that requester or data subject to remove the grounds for refusal;
 - given the requester or data subject a reasonable opportunity to seek such assistance;
 - as far as reasonably possible, furnished the requester or data subject with any information that would assist the making of the request in the prescribed form; and
 - given the requester a reasonable opportunity to confirm the request or alter it to comply with section 18 of PAIA or 24 of POPIA.
- 6.1.3 working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body. For example-
- 6.1.3.1 the responsible party must obtain prior authorisation from the Regulator pertaining to the following:
- processing of any unique identifiers of data subjects;
 - processing of information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;
 - processing of information for the purposes of credit reporting; and
 - transfer of special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 724. 6.1.3.2 pending the authorisation⁵ or completion of investigation⁶ by the Regulator, or until such time the responsible party receives a notice⁷ that a more detailed investigation will not be conducted, the responsible party is prohibited from carrying out information processing. This means that processing that falls under paragraph
- 6.1.3.1 above is automatically suspended pending the authorisation from the Regulator.
- 6.1.3.3 failure to notify the Regulator of the processing listed above is an offence and upon conviction, the responsible party will be liable to a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment⁸.
- 6.1.4 otherwise ensuring compliance by a body with the provisions of this POPIA. For example-
- 6.1.4.1 POPIA prescribes eight (8) conditions for the lawful processing of personal information⁹ by or for a responsible party and it is the responsibility of an Information Officer to ensure compliance with those conditions.



- 6.2 *The additional duties and responsibilities of the Information Officers, in terms of regulation 4 of POPIA, are to ensure that-*
- 6.2.1 *a compliance framework is developed, implemented, monitored and maintained;*
 - 6.2.2 *a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;*
 - 6.2.3 *a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA, as amended;*
 - 6.2.4 *internal measures are developed together with adequate systems to process requests for information or access thereto;*
 - 6.2.5 *internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator; and*
 - 6.2.6 *upon request by any person, copies of the manual are provided to that person upon the payment of a fee to be determined by the Regulator from time to time.*
- 6.3 *The Information Officer of each public body must annually, and in terms of section 32 of PAIA, submit to the Regulator a report regarding-*
- 6.3.1 *the number of requests for access received;*
 - 6.3.2 *the number of requests for access granted in full;*
 - 6.3.3 *the number of requests for access granted in terms of section 46;*
 - 6.3.4 *the number of requests for access refused in full and refused partially and the number of times each provision of this Act was relied on to refuse access in full or partially;*
 - 6.3.5 *the number of cases in which the periods stipulated in section 25(1) were extended in terms of section 26 (1);*
 - 6.3.6 *the number of internal appeals lodged with the relevant authority and the number of cases in which, as a result of an internal appeal, access was given to a record;*
 - 6.3.7 *the number of internal appeals which were lodged on the ground that a request for access was regarded as having been refused in terms of section 27;*
 - 6.3.8 *the number of applications to a court which were lodged on the ground that an internal appeal was regarded as having been dismissed in terms of section 77 (7).*
- 6.4 *The Regulator may request an Information Officer of a private body, in terms of section 183(4), to furnish to the Regulator with the information listed in paragraph 6.3 above.*
- 6.5 *If, after being given access to the record concerned, the health practitioner consulted in terms of subsection (1) is of the opinion that the disclosure of the record to the relevant person would be likely to cause serious harm to his or her physical or mental health, or well-being, the information officer may only give access to the record if the requester proves to the satisfaction of the information officer that adequate provision is made for such counselling or arrangements as are reasonably practicable before, during or after the disclosure of the record to limit, alleviate or avoid such harm to the relevant person¹⁰.*
- 6.6 *Registration of Information Officers¹¹ with the Regulator is not only the prerequisite for Information Officer to take up their duties in terms of POPIA and PAIA, but is a compulsory requirement for every person identified in paragraph 5.1 above.*