



FREQUENTLY ASKED QUESTIONS ABOUT POPIA WITH ANSWERS

INDEX

CROSS BORDER TRANSFER OF PERSONAL INFORMATION	2
CONFLICTING LAWS	3
FURTHER PROCESSING	4
KEEPING INFORMATION UP TO DATE	6
REFERRALS AND CONSENT	7
SECTION 18 PROCESSING NOTICES	9
SECURITY OF DATA	12
OPERATORS	16
BANKING DETAILS	18
DATA BREACH	20
RIGHTS TO PERSONAL INFORMATION	22
SPECIAL PERSONAL INFORMATION	24
Section 26 - Prohibition on processing of Special Personal Information	24
Section 27 - General authorisation concerning Special Personal Information	24
Section 28 - Authorisation concerning Data Subject's religious or philosophical beliefs	24
Section 29 - Authorisation concerning Data Subject's race or ethnic origin	24
Section 30 - Authorisation concerning Data Subject's trade union membership	24
Section 31 - Authorisation concerning Data Subject's political persuasion	24
RIGHT TO CORRECT PERSONAL INFORMATION	34
INFORMATION OFFICERS	36



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
<p>1 CROSS BORDER TRANSFER OF PERSONAL INFORMATION</p>		
<p>Can the Responsible Party send Personal Information of a Data Subject cross border?</p>	<p>The Act does not allow the Responsible Party to send Personal Information offshore or cross border into other countries unless the receiving country has the same level of protection in respect of Personal Information as per its respective Data privacy laws which are applicable and in place in that receiving country.</p> <p>The South African Act covers and protects Personal Information belonging to Individuals and to legal entities. POPIA is one of the more progressive laws in respect of Data protection in the world.</p> <p>Most cross-border countries' Data protection laws apply to individuals only and not to legal entities. In consequence, most cross border countries or jurisdictions do not have as strong a set of Data privacy laws in place.</p> <p>Following this, in terms of POPIA, a Responsible Party may not send Personal Information to another country unless the same level of protection <i>vis-a vis</i> personal Data is provided in such country to the Data Subject.</p> <p>As a result, if Personal Information is sent across border, a Responsible Party must first ascertain if there are data protection laws applicable in that receiving country, and if so, what the laws state and if they apply to an individual and to an entity.</p> <p>If the level of protection is less favourable than that housed under POPIA, the Responsible Party has to get consent from the Data Subject to send the Personal Information to such country, alternatively, the Responsible Party must conclude a binding corporate agreement or an agreement with the receiving entity in terms of which such entity agrees and undertakes to comply with the South African Data privacy laws i.e. POPIA.</p>	<p>Ascertain if and where Personal Information is sent outside RSA.</p> <p>List this under the Cross-Border PI Register.</p> <p>Ascertain what Data protection laws apply in the receiving entity's country and whether these are on a par or better than POPIA.</p> <p>If not, ensure that the Data Subject is advised of this fact and that consent to send the Personal Information is received despite the inadequate level of protection or that a contract is concluded as between the Responsible Party and the recipient of the Data Subjects' PI where the recipient undertakes to comply in all respects with POPIA.</p> <p>Indemnities from the recipient of the Personal Information should be obtained in the case of a breach of its contractual obligations to comply with POPIA.</p> <p>TO MANAGE THE RISK OF NON-COMPLIANCE, ALL CROSS-BORDER FLOWS OF PI MUST BE ACCOMPANIED WITH A DATA TRANSFER AGREEMENT.</p> <p>SEE STANDARD DATA TRANSFER AGREEMENT WHICH HAS TO BE CONCLUDED WITH RECIPIENT OF ANY PI.</p>



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
<p>2 CONFLICTING LAWS</p>		
<p>If there is another law applicable in South Africa which pertains to the processing of Personal Information, which law will take precedent – POPIA or the other law?</p>	<p>Section 3 - Application and interpretation of Act found under POPIA does cover what will happen when there is another law which provides or regulates the use of Personal Information, and which law will take precedent.</p> <p>This provision reads as follows:</p> <p><i>“This Act applies to the exclusion of any provision of any other legislation that regulates the processing of Personal Information and that is materially inconsistent with an object, or a specific provision, of this Act.</i></p> <p><i>If any other legislation provides for conditions for the lawful processing of Personal Information that are more extensive than those set out in Chapter 3, the extensive conditions prevail.</i></p> <p><i>This Act must be interpreted in a manner that gives effect to the purpose of the Act set out in section 2; and does not prevent any public or private body from exercising or performing its powers, duties and functions in terms of the law as far as such powers, duties and functions relate to the processing of Personal Information and such processing is in accordance with this Act or any other legislation, that regulates the processing of Personal Information.”</i></p> <p>Following this, where an Act provides for more detailed or extensive processing provisions then that Act and its more extensive processing provisions must be applied, so long as it is not materially inconsistent with an object, or a specific provision, of POPIA.</p>	<p>ACTION:</p> <ol style="list-style-type: none"> 1. List all laws which apply to the Responsible Party which regulate or refer to the processing of Personal Information. 2. List the relevant sections under the Act which regulate or refer to the processing of Personal Information. 3. List the conflicting or similar provisions found under POPIA. 4. Determine which takes precedent by ascertaining which Act or law provides for more detailed or extensive processing provisions, and which is not materially inconsistent with an object or a specific provision of POPIA. 5. Apply the Act or provision which provides for the more extensive processing provisions. <p>SEE CONFLICTING LAWS REGISTER</p>



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
3	FURTHER PROCESSING	
<p>What is “further processing”?</p>	<p>Further processing of Personal Information is where processing of a Data Subject’s Personal Information is done in accordance or in a manner compatible with the purpose for which the original information was collected in terms of POPIA.</p> <p>Example of Further Processing</p> <p>Further processing of employees’ Personal Information is in compliance with the law i.e., processing for South African Revenue Services, deduction of union membership as per the LRA, Garnishee, EAP and Risk pool in terms of the OHSA.</p> <p>To assess whether further processing is compatible with the purpose of collection, the Responsible Party must take account of—</p> <ul style="list-style-type: none"> • the relationship between the purpose of the intended further processing and the purpose for which the information has been collected; • the nature of the information concerned; • the consequences of the intended further processing for the Data Subject; • the manner in which the information has been collected; and • any contractual rights and obligations between the parties. • the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to public health or public safety; or the life or health of the Data Subject or another individual; 	<p>SECTION 15 - FURTHER PROCESSING TO BE COMPATIBLE WITH PURPOSE OF COLLECTION</p> <p>Ensure that:</p> <p>Further processing of information is in line with the purpose for which the Personal Information was originally collected.</p> <p>Personal Information is further processed for similar purposes for which it was collected.</p> <p>Prior consent is obtained from the Data Subject before further processing occurs, or place <i>Right to Further Processing</i> in consent form.</p> <p>The section 18 processing notice should stipulate that the Data Subject’s Personal Information may be further processed.</p> <p>Training and awareness in place on requirements for further processing.</p>

- the information is used for historical, statistical or research purposes and the Responsible Party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or
- the further processing of the information is in accordance with an exemption granted under POPIA.

The further processing of Personal Information is not incompatible with the purpose of collection if:

- the Data Subject, or a competent person where the Data Subject is a child, has consented to the further processing of the information;
- the information is available in or derived from a public record or has deliberately been made public by the Data Subject;
- further processing 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 with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
- for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
- in the interests of national security.



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
4	KEEPING INFORMATION UP TO DATE	
<p>Does the Responsible Party have a duty to keep Personal Information up to date?</p> <p>How will I do this?</p>	<p>Steps to ensure that information is correct</p> <p>A Responsible Party must take reasonably practicable steps to ensure that the Personal Information is complete, accurate, not misleading and updated where necessary.</p> <p>In taking the steps the Responsible Party must have regard to the purpose for which Personal Information is collected or further processed.</p>	<p>SECTION 16 - QUALITY OF INFORMATION</p> <p>The Responsible Party must ensure that Personal Information of all Data Subjects is kept up to date, complete, not misleading and accurate.</p> <p>Conduct ongoing due diligence when processing Personal Information to ensure that only quality information is processed and recorded.</p> <p>Ensure updates are given effect to.</p> <p>Ensure that Data Subject is given an opportunity to update information using prescribed format under Regulations.</p> <p>Place right and onus to keep details up to date under Section 18 Processing Notice</p> <p>Send out a regular update form to Data Subjects.</p> <p>SEE UPDATE FORM</p>



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
5	REFERRALS AND CONSENT	
<p>Can I make use of another’s Personal Information if this has been provided to me by another Data Subject?</p> <p>How will I handle a reference placed in a CV?</p> <p>What must I do if I am contacted by a person asking to verify a Data Subject’s details or salary, or employment and performance?</p>	<p>You may only use another’s Personal Information if they give you consent to use or process it or where:</p> <p>Processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is party;</p> <p>Processing complies with an obligation imposed by law on the Responsible Party;</p> <p>Processing protects a legitimate interest of the Data Subject;</p> <p>Processing is necessary for the proper performance of a public law duty by a public body; or</p> <p>Processing is necessary for pursuing the legitimate interests of the Responsible Party or of a third party to whom the information is supplied.</p> <p>Responsible Party to obtain consent</p> <p>The Responsible Party bears the burden of proof for the Data Subject’s or competent person’s consent.</p> <p>Withdraw consent</p> <p>The Data Subject or competent person may withdraw his, her or its consent at any time: Provided that the lawfulness of the processing of Personal Information before such withdrawal or the processing of Personal Information will not be affected.</p> <p>Object</p> <p>A Data Subject may object, at any time, to the processing of Personal Information:</p>	<p>SECTION 11 - CONSENT, JUSTIFICATION AND OBJECTION</p> <ol style="list-style-type: none"> 1. Ensure that consent is obtained from the Data Subject prior to processing of Personal Information and that such consent is retained as proof and that such Data Subject is given a Section 18 Notice, alternatively make sure that where consent is not required, that a carve-out will apply to such collection. 2. Always ensure that a person providing you with a referral has permission to pass this detail onwards and that the owner has expressly been made aware of the sharing of his, her or its details and the reasons why this detail was shared. 3. CV referrals must no longer consist of a name or reference or contact number. Instead, the reference must write a referral letter and, in such letter, give the Responsible Party the consent to use his or her details. 4. Never confirm person’s details such as salary or employment performance history unless that person has given written permission to share and divulge such details. <p>SEE VARIOUS PROCESSING NOTICES, ESPECIALLY THE HR PROCESSING NOTICE</p> <p>WHEN TRANSFERRING PI TO ANOTHER, MAKE USE OF THE STANDARD ONWARDS TRANSMISSION NOTICE</p>



	<p>(a) In the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or</p> <p>(b) For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.</p> <p>If a Data Subject has objected to the processing of Personal Information, the Responsible Party may no longer process the Personal Information.</p>	
--	--	--



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
6	SECTION 18 PROCESSING NOTICES	
<p>What is a section 18 Informed Notice and why is it required?</p>	<p>Confirmation from Data Subject</p> <p>If Personal Information is collected, the Responsible Party must take reasonably practicable steps to ensure that the Data Subject is aware of—</p> <ul style="list-style-type: none"> • the information being collected and where the information is not collected from the Data Subject, the source from which it is collected; • the name and address of the Responsible Party; • the purpose for which the information is being collected; • whether or not the supply of the information by that Data Subject is voluntary or mandatory; • the consequences of failure to provide the information; • any particular law authorising or requiring the collection of the information; • the fact that, where applicable, the Responsible Party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation; • any further information such as the - recipient or category of recipients of the information; nature or category of the information; existence of the right of access to and the right to rectify the information collected; 	<p>SECTION 18 - NOTIFICATION TO DATA SUBJECT WHEN COLLECTING PERSONAL INFORMATION</p> <p>To comply with these section 18 requirements, which is one of the more important parts of the Act, the Responsible Party must compile a section 18 Data Processing Notices, which must be specific and apply to a specific category of Data Subject(s), i.e. an employee or student.</p> <p>Below are the steps which should be followed to prepare and implement a section 18 notification process:</p> <ol style="list-style-type: none"> 1. Ascertain who the Data Subjects are; 2. Ensure that all Data Subjects are informed of their rights as directed under section 18; 3. Data Subjects are told why the Personal Information is being processed; 4. Data Subjects are informed about the purpose for which the information is collected; 5. In the recruitment or student enrolment or vendor enrolment process, explanation is provided as to why consent forms need to be signed in respect of verification exercises such as background checks etc. and Data Subjects must be advised that if no consent is provided for credit and/or criminal record checks it could count against the Data Subject; 6. Data Subjects should be notified of the consequences of providing incorrect Personal Information or failing to provide consent to processing. 7. Ensure that the Data Subject is always informed of the collection of Personal Information and the purpose; 8. Ensure that the Data Subject is provided with all relevant information of the Responsible Party and actions associated with the collection of the PI; 9.

- existence of the right to object to the processing of Personal Information as referred to in POPIA; and the Right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the Data Subject to be reasonable.

Timing

The steps referred to above must be taken—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; or in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

10. Business documents, agreements and consent forms must be reviewed and amended to contain relevant business information and section 18 disclosures;
11. Various consent forms used to collect Personal Information must be filed and saved and the procedure for dealing with these consent forms must be indicated in the approved and signed-off SOP;
12. Awareness of exemptions under section 18(1) – 18(4) where consent not required;
13. Training and awareness must take place on the section 18 requirements;
14. SOP to be developed for section 18(1) – 18(4) procedures;
15. Consent must always be received, as a first resort, and in an effort to participate in best practise;
16. Consider a section 18 “disclosure section” in all documents;
17. **Ensure awareness of when a section 18 notice does not have to be provided;**
18. **Unpack not necessary to comply with provisions.**

It is not necessary for a Responsible Party to comply with the above if —

- the Data Subject, or a competent person where the Data Subject is a child, has provided consent for the non-compliance;
- non-compliance would not prejudice the legitimate interests of the Data Subject as set out in terms of this Act;
- non-compliance is necessary — (i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences; (ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997); (iii) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or (iv) in the interests of national security;

		<ul style="list-style-type: none">• compliance would prejudice a lawful purpose of the collection;• compliance is not reasonably practicable in the circumstances of the particular case; or• 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. <p>SEE THE STANDARD SECTION 18 PROCESSING NOTICES</p>
--	--	---



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
7	SECURITY OF DATA	
<p>What steps does a Responsible Party have to take to protect the Personal Information under its care?</p> <p>What steps does an Operator acting on behalf of the Responsible Party have to take to protect the Personal Information under its care?</p>	<p>A Responsible Party as well as an Operator 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:</p> <p>(a) loss of, damage to or unauthorised destruction of Personal Information; and</p> <p>(b) unlawful access to or processing of Personal Information.</p> <p>To give effect to the above, the Responsible Party must take reasonable measures to—</p> <p>(a) identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;</p> <p>(b) establish and maintain appropriate safeguards against the risks identified;</p> <p>(c) regularly verify that the safeguards are effectively implemented; and</p> <p>(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.</p> <p>The Responsible Party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.</p>	<p>SECTION 19 - SECURITY MEASURES ON INTEGRITY AND CONFIDENTIALITY OF PERSONAL INFORMATION</p> <p>To ensure that Personal Information is secured and is treated with integrity and is always kept confidential, the Responsible Party must ensure that the Personal Information is safeguarded.</p> <p>The provisions of this section are vague and do not give direction.</p> <p>Below are some detailed steps and actions, which Responsible Party must take to ensure that the Personal Data which it holds is correctly stored and safeguarded.</p> <p>Records of Personal Information will include all personnel information held by the Responsible Party as well as other records for which the Responsible Party is responsible for but which are being held and processed by a third-party record such as employment agency & recruitment records, RICA Documents, interview files, outsourced Time and Attendance records, sick leave certificates held by clinics, disciplinary information, talent management system, contracts, vendor documents, marketing Data bases etc.</p> <p>Develop Personal Information Protection Security Procedure and related controls</p> <p>In order to implement a <i>security of Data compliance programme</i> ensure that the following controls are considered, devised and implemented:</p> <ol style="list-style-type: none"> 1. Ascertain all types of Personal Information which the Responsible Party and its third parties and Operators have in their possession. 2. List this under a process mapping exercise. 3. Classify the Data and records in accordance with the Responsible Party Data Management Classification System.

		<ol style="list-style-type: none"> 4. Develop Records Management Policy and procedures. 5. Ensure that Physical Personal Information is stored in locked cabinets and access-controlled offices. 6. Identity and access controls must be implemented and monitored regularly in respect of access to all Personal Data. 7. Perform proper information backups on all Personal Information to ensure availability and integrity of Personal Information. 8. Implement where applicable adequate change control procedures and adequate restrictions to systems (SAP). 9. Arrange for regular IT security audits of all IT platforms and systems by third parties. 10. Conclude Operator or third-party contracts with Contracts with Data Storage service providers contract (cloud computing, servers and Metro file), which outlines the security measures, which they must implement in terms of the storage and confidentiality of Personal Information and obtain strong indemnities in the case of any breach. 11. Where Personal Information is stored in paper files and in filing rooms or stores ensure that such files are housed or kept under lock and key and rooms are fire and waterproof. 12. Ensure access control - access to Personal Information is given on a need to know only basis, approved by line managers. 13. Ensure access to all servers is limited. 14. Ensure back-ups of Personal Information stored in all areas is conducted regularly. 15. Ensure Business Contingency Management (BCM) in place which stipulates what should be done in cases of emergencies including data breach. 16. Ensure adequate controls in place to prevent and IT systems from hackers and unauthorised access and the protection complies with the IT policy.
--	--	---

		<p>17. Mitigation measures include authorisations and access control (single sign-on)</p> <p>18. Perform external quarterly audits on the Responsible Party systems</p> <p>19. Make sure that audit findings and corrective controls get resolved timeously.</p> <p>20. Non-disclosure agreements to be signed by all employees and Operators or third parties who receive Personal Information from the Responsible Party – see employment contract and Operator clauses to ensure that this requirement has been implemented.</p> <p>21. Ensure that standard clauses are included in employment contracts ensuring confidentiality of personnel information and employee has obligation to safeguard all information under its control.</p> <p>22. Manage personnel file movements to and from storerooms – ensure process is in place where employee signs file in and out.</p> <p>23. HR personnel files in open plan workstations to be safeguarded – implement a clean desk policy. No personnel information should be left on desks, whether in open plan or in closed office.</p> <p>24. Access to the systems housing Personal Information is closely monitored</p> <p>25. Limited access on a need-to-know basis to documents on share-point per portfolio.</p> <p>26. Training and awareness to be conducted covering the requirements of safety, integrity and confidentiality of Personal Information.</p> <p>27. Requirements of integrity and confidentiality contained in the POPIA policy and SOPs.</p> <p>28. IT systems are to be configured to ensure that the integrity and confidentiality of information is not compromised.</p> <p>29. Confidentiality clauses must be contained in business documents and agreements, but which give effect to section 11 of POPIA.</p> <p>30. Ensure Retention and disposal of Personal Information done strictly in terms of the Records Management Policy.</p>
--	--	---

		<p>31. Access to all servers is tight in that it is password protected and restricted to certain users.</p> <p>32. The risk assessment on identified risk gets updated or revised annually.</p> <p>33. Employees are allowed to view their personnel file but not allowed to remove the file from the storage area and access is restricted to this area.</p> <p>34. Documents are password protected and encrypted.</p> <p>35. Limited and restricted access to student and personnel files storage area and controls reviewed on ongoing basis.</p> <p>36. The HR administrators have a register to log details of persons who have access to the file.</p> <p>37. The password control for access to systems reviewed regularly.</p> <p>38. All departments should manage use of printers.</p> <p>39. Identity and access controls must be implemented and monitored regularly.</p> <p>40. Proper information backups to ensure availability and integrity of Personal Information.</p> <p>41. Change control procedures and adequate restrictions to systems (SAP)</p> <p>42. Continued review and revision of short comings</p> <p>43. Records Management Policy and Information Classification Policy reviewed and updated regularly.</p> <p>44. Develop a plan for conducting audits on generally accepted information security practices in order to ensure compliance with the requirements of section 19(3)</p> <p>45. Develop an audit plan on generally accepted information security practices.</p> <p>SEE THE CHECKLIST ON DATA MANAGEMENT PROCEDURES TO BE COMPLETED BY THE RESPONSIBLE PARTY'S IT</p>
--	--	--



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
8	OPERATORS	
<p>Who is an Operator?</p> <p>What are the responsibilities of an Operator?</p> <p>What is an Operator Agreement?</p>	<p>An Operator is any person or entity that processes Personal Information on behalf of a Responsible Party such as the Responsible Party.</p> <p>An Operator or anyone processing Personal Information on behalf of a Responsible Party or an Operator, must:</p> <ul style="list-style-type: none"> • process such information only with the knowledge or authorisation of the Responsible Party; and • treat Personal Information, which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties. <p>A Responsible Party must, in terms of a written contract between the Responsible Party and the Operator, ensure that the Operator which processes Personal Information for the Responsible Party establishes and maintains the security measures referred to in POPIA.</p> <p>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.</p> <p>An Operator Agreement is an agreement which will be concluded with an Operator which sets out the Operator’s duties in relation to the processing of Personal Information on behalf of the Responsible Party (the Responsible Party).</p>	<p>SECTION 20 - INFORMATION PROCESSED BY OPERATOR OR PERSON ACTING UNDER AUTHORITY</p> <p>SECTION 21 - SECURITY MEASURES REGARDING INFORMATION PROCESSED BY OPERATOR</p> <p>Develop a list of all Operators, which are used.</p> <p>Insert details into Operator Register</p> <p>Develop a standard Operator Agreement and Data Security SLA</p> <p>Develop a notification of security breach notice and reporting guide.</p> <p>Note that an Operator or anyone processing Personal Information on behalf of the Responsible Party:</p> <ul style="list-style-type: none"> • must process such information only with the knowledge or authorisation of the Responsible Party; and • must treat Personal Information which comes to their knowledge as confidential; and • must not disclose it, unless required by law or in the course of the proper performance of their duties. <p>The Responsible Party must, in terms of a written contract between it and the Operator, ensure that the Operator which processes Personal Information for the Responsible Party establishes and maintains the security measures referred to in POPIA.</p> <p>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.</p>



All employees must ensure that an Operator Agreement is concluded with all Operators, using the standard the Responsible Party Operator Template and SLA setting out the IT security measures which have to be taken and implemented by the Operator when processing and storing the Responsible Party's Data Subjects' Personal Data on its behalf.

SEE OPERATOR REGISTERS AND OPERATOR AGREEMENTS



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
9	BANKING DETAILS	
<p>What are a Responsible Party's duties in connection with a Data Subject's banking details?</p> <p>What is an account number?</p> <p>What are a third party's duties in connection with a Data Subject's banking details?</p>	<p>All Responsible Parties who hold or who are in possession of a person's banking details and who uses these banking details for whatever reasons, has a duty to safeguard these details.</p> <p>A Responsible Party who contravenes these provisions is guilty of an offence.</p> <p>The contravention however must be of a serious or persistent nature; and likely cause substantial damage or distress to the Data Subject.</p> <p>Furthermore, the Responsible Party must have known or ought to have known that there was a risk that the contravention would occur; or such contravention would likely cause substantial damage or distress to the Data Subject; and have failed to take reasonable steps to prevent the contravention.</p> <p>If a Responsible Party is charged with such an offence as set out above, it is a valid defence to such a charge to contend that he or she has taken all reasonable steps to comply with the provisions of section 8 and that it has lawfully processed such banking details in accordance with POPIA, including the implementation of safeguards and security measures as per section 19 of POPIA.</p> <p>"Account number", for purposes of this section and section 106, means any unique identifier that has been assigned—</p> <p>(a) to one Data Subject only; or</p> <p>(b) jointly to more than one Data Subject,</p> <p>by a financial or other institution, which enables the Data Subject, referred to in paragraph (a), to access his, her or its own funds or to access credit facilities or which enables a Data Subject, referred to in paragraph (b), to access joint funds or to access joint credit facilities.</p>	<p>SECTION 105 - UNLAWFUL ACTS BY RESPONSIBLE PARTY IN CONNECTION WITH ACCOUNT NUMBER</p> <p>SECTION 106 - UNLAWFUL ACTS BY THIRD PARTIES IN CONNECTION WITH ACCOUNT NUMBER.</p> <p>Ascertain what bank account details the Responsible Party holds on behalf of Data Subjects.</p> <p>Ensure advanced security measures are in place to protect these details and only authorised persons have access to such information.</p> <p>Note the responsibilities and duties of a third party and its defences should it be charged with criminal conduct.</p>

Any third party who knowingly or recklessly, and without the consent of the Responsible Party obtains or discloses an account number of a Data Subject; or procures the disclosure of an account number of a Data Subject to another person is guilty of an offence.

Whenever such a person is charged with an offence set out above, it is a valid defence to such a charge to contend that—

- (a) the obtaining, disclosure or procuring of the account number was necessary for the purpose of the prevention, detection, investigation or proof of an offence; or required or authorised in terms of the law or in terms of a court order;
- (b) he or she acted in the reasonable belief that he or she was legally entitled to obtain or disclose the account number or, as the case may be, to procure the disclosure of the account number to the other person;
- (c) he or she acted in the reasonable belief that he or she would have had the consent of the Responsible Party if the Responsible Party had known of the obtaining, disclosing or procuring and the circumstances of it; or
- (d) in the particular circumstances the obtaining, disclosing or procuring was in the public interest.



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
10 DATA BREACH		
<p>What must one do in the case of a data breach?</p> <p>What must the data breach notification state?</p> <p>Who must be notified and how?</p>	<p>A data breach is when a Data Subject’s Personal Information has been accessed unlawfully or in an unauthorised manner or where the information has been lost or destroyed contrary to the provisions of POPIA.</p> <p>In the case of such a Data breach, i.e. where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person, the Responsible Party must notify the Regulator and, subject to the below, the Data Subject, unless the identity of such Data Subject cannot be established.</p> <p>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.</p> <p>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 Regulator determines that notification will impede a criminal investigation by the public body concerned.</p> <p>The notification to a Data Subject must be in writing and communicated to the Data Subject in at least one of the following ways:</p> <p>(a) mailed to the Data Subject’s last known physical or postal address;</p>	<p>SECTION 22 - NOTIFICATION OF SECURITY COMPROMISES</p> <p>To comply with section 22 and to ensure that the Regulator, as well as the owner of the information or Data Subject, is aware of the breach, the Responsible Party must implement the following controls:</p> <ol style="list-style-type: none"> 1. Implement processes to identify security breaches and corresponding processes whereby the Responsible Party notifies the Regulator and Data Subject of the breach: 2. Information Regulator must be informed about the security breach. 3. Data Subjects must be informed about the security breach. 4. The Information Officer needs to establish a process that will provide guidance on how this should be addressed or handled. 5. When there are reasonable grounds to believe that there might have been a security breach, a communique ought to be distributed to the Data Subjects informing them of the occurrence, the responsible individual and this requirement to be included in the Service Level Agreements. 6. Ensure that there are procedures in place to report breach of security to the Regulator and a Data Subject. 7. Development of a SOP document which dictates compliance with these requirements 8. Training and awareness sessions on the requirements herein. 9. HR to notify employees immediately when personnel files go missing to alert the employees and to get them to assist in reconstructing the file.

	<ul style="list-style-type: none"> (b) sent by e-mail to the Data Subject’s last known e-mail address; (c) placed in a prominent position on the website of the Responsible Party; (d) published in the news media; or (e) as may be directed by the Regulator. <p>The notification must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including:</p> <ul style="list-style-type: none"> (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; and (d) if known to the Responsible Party, the identity of the unauthorised person who may have accessed or acquired the Personal Information. <p>The Regulator may direct a Responsible Party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of Personal Information, if the Regulator has reasonable grounds to believe that such publicity would protect a Data Subject who may be affected by the compromise.</p>	<p>10. Information Regulator must be informed about the security breach to get direction on how to tackle the security breach and the Data Subjects informed.</p> <p>11. Notification must cover the following items:</p> <p>Sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including:</p> <ul style="list-style-type: none"> (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 about the measures to be taken by the Data Subject to mitigate the possible adverse effects of the security compromise; and (d) if known to the Responsible Party, the identity of the unauthorised person who may have accessed or acquired the Personal Information. <p>12. The most efficient means of communication to be utilised both internal and external to send the message across timeously, i.e. internal communique to be distributed, SMS, press and media release and statements etc.</p> <p>13. Develop Personal Information Protection Security Procedure.</p> <p>14. Wherever there is a suspected case of security concern, employees are made aware via internal communique, i.e. through e-mail.</p> <p>REFER TO THE DATA BREACH PROVISIONS IN THE RESPONSIBLE PARTY’S POPIA POLICIES</p>
--	---	---



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
11 RIGHTS TO PERSONAL INFORMATION		
<p>What is a Data Subject's right to ask for its Personal Information?</p> <p>How must this request be made?</p>	<p>Note that the provisions of sections 18 and 53 of the Promotion of Access to Information Act (PAIA) apply to requests made for access to one's Personal Information in terms of section 23 of POPIA.</p> <p>In order to ask for such access and information, a Data Subject, having provided adequate proof of identity, has the right to request a Responsible Party to confirm, free of charge, whether or not the Responsible Party holds Personal Information about the Data Subject; and request from a Responsible Party the record or a description of the Personal Information about the Data Subject held by the Responsible Party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information:</p> <ul style="list-style-type: none"> (i) within a reasonable time; (ii) at a prescribed fee, if any; (iii) in a reasonable manner and format; and (iv) in a form that is generally understandable. <p>Note: If, in response to a request in terms of the above, Personal Information is communicated to a Data Subject, the Data Subject must be advised of the right in terms of POPIA to request the correction of information.</p> <p>Note further that a Responsible Party under PAIA may require the Data Subject to pay a fee to process such Personal Information.</p>	<p>SECTION 23 - ACCESS TO PERSONAL INFORMATION</p> <p>SECTION 25 - MANNER OF ACCESS</p> <p>To ensure that a Data Subject has the right to request access to his/her/its Personal Information, the Responsible Party must implement the following controls:</p> <ol style="list-style-type: none"> 1. PAIA manual to be enhanced with POPIA provisions; 2. PAIA process in place and accessible via the Responsible Party website which sets out how one may ask to access Personal Information; 3. Reference to rights to Personal Information access in section 18 Processing Notice; 4. Appointment of an Information Officer to deal with these requests and related requirements; 5. Employees are aware that Data Subjects, including all employees, may ask for personal details held by the Responsible Party, and that such request must be done using the PAIA procedure, 6. Training and awareness on how Personal Information may be asked for and accessed and, where applicable, rectified, 7. Develop protocols for engaging with Data Subjects and scope of information / confirmations that may be allowed. <p>REFER TO THE RESPONSIBLE PARTY'S PAIA MANUAL AND PAIA PROCEDURE</p>

If a Data Subject is required by a Responsible Party to pay a fee for services provided to the Data Subject in terms of the above to enable the Responsible Party to respond to a request, the Responsible Party must give the applicant a written estimate of the fee before providing the services; and may require the applicant to pay a deposit for all or part of the fee.

Note that a Responsible Party may or must refuse to disclose any information requested in terms of the above to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act apply.

Also note that the provisions of sections 30 and 61 of the Promotion of Access to Information Act are applicable in respect of access to health or other records.

If a request for access to Personal Information is made to a Responsible Party and part of that information may or must be refused in terms of the above, every other part must be disclosed.



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
12 SPECIAL PERSONAL INFORMATION	<p>The Act distinguishes between Special Personal Information and Personal Information.</p> <p>Special Personal Information (SPI) is sensitive information pertaining to a person or entity, which could cause greater harm if exposed or accessed without the Data Subject’s permission compared to Personal Information.</p> <p>Special Information includes:</p> <p>(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; or</p> <p>(b) the criminal behavior of a Data Subject to the extent that such information relates to the alleged commission by a Data Subject of any offence; or any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.</p> <p>Whilst the Act under section 29 prohibits the processing of Special Information, to ensure that this right is balanced with other rights, such as the rights of medical service providers and hospitals, it does allow certain Responsible Parties to process SPI with the prior consent of the Data Subject or alternatively, without consent under certain conditions and circumstances.</p> <p>These are explained below.</p>	<p>Section 26 - Prohibition on processing of Special Personal Information</p> <p>Section 27 - General authorisation concerning Special Personal Information</p> <p>Section 28 - Authorisation concerning Data Subject’s religious or philosophical beliefs</p> <p>Section 29 - Authorisation concerning Data Subject’s race or ethnic origin</p> <p>Section 30 - Authorisation concerning Data Subject’s trade union membership</p> <p>Section 31 - Authorisation concerning Data Subject’s political persuasion</p> <ol style="list-style-type: none"> 1. Understand what is Special Personal Information (SPI). 2. Ascertain and list the SPI which the Responsible Party processes and the reasons why it is needed and required and whether it is necessary. 3. List all SPI under a SPI register with corresponding reasons why the SPI is processed. 4. Ensure reference to such SPI and the reasons why it is required, is inserted under the relevant section 18 Processing Notice and where possible, consent to such processing obtained. 5. Apply for an Exemption if processing is in the Public Interest.



26 - PROHIBITION ON PROCESSING OF SPECIAL PERSONAL INFORMATION

A Responsible Party may, subject to POPIA, 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; or
- (b) the criminal behavior of a Data Subject to the extent that such information relates to the alleged commission by a Data Subject of any offence; or any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

27 - GENERAL AUTHORISATION CONCERNING SPECIAL PERSONAL INFORMATION

The prohibition on processing Personal Information, as referred to in POPIA, **does not apply if the—**

- (a) processing is carried out with the consent of a Data Subject;
- (b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- (c) processing is necessary to comply with an obligation of international public law;
- (d) processing is for historical, statistical or research purposes to the extent that— (i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or (ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;
- (e) information has deliberately been made public by the Data Subject; or
- (f) provisions of POPIA are, as the case may be, complied with.

The Regulator may, upon application by a Responsible Party and by notice in the Gazette, authorise a Responsible Party to process special Personal Information if such processing is in the public interest and appropriate safeguards have been put in place to protect the Personal Information of the Data Subject.

The Regulator may impose reasonable conditions in respect of any authorisation granted as set out above.

To process Special Personal Information, the Responsible Party should take note of the various requirements and carve outs to the out and out prohibition of processing Special Personal Information.

Following this the Responsible Party must educate all employees on what amounts to Special Personal Information (SPI) and the limitations on the processing of such SPI as well as when SPI can or may be processed and the conditions which must be shown to legitimise such processing. To ensure that Special Personal Information is processed lawfully the Responsible Party should put the following controls in place:

1. Ascertain what special Personal Information is processed by the Responsible Party and insert this into a Special Personal Information Register.
2. Determine if this information is necessary for the required purpose and the reason why it is needed.
3. Processing of SPI may only happen with the consent from the Data Subject, so ensure that consent from the Data Subject is obtained. This can be inserted under the relevant section 18 Processing Notice.
4. Ensure that the relevant section 18 Processing Notices include references to SPI where applicable.
5. If consent is not obtained, ensure that there is a sound reason permitted under POPIA to process the Special Personal Information.
6. List the reasons where processing of Special Personal Information is permitted without a Data Subject's consent, being:
 - processing is necessary for the establishment, exercise or defence of a right or obligation in law;
 - processing is necessary to comply with an obligation of international public law;
 - processing is for historical, statistical or research purposes to the extent that—
 - (i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or

(ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;

- information has deliberately been made public by the Data Subject; or
- provisions of POPIA are, as the case may be, complied with.

7. Only process Special Personal Information if it is in terms of an obligation in law, i.e. employment equity analysis, trade union membership, criminal reference checks, health or sex life, medical assessments or as permitted above or under sections 26-35 of POPIA.
8. Manage Data processing collection forms and delete reference to SPI where not necessary.
9. where SPI is processed – document reason why it was needed and get Data Subject to sign the consent and reasons form.
10. Develop a Special Personal Information Processing Procedure.
11. Implement the approved Special Personal Information Protection Security Procedure
12. Apply for an exemption where necessary – to be done by Information Officer.
13. Training and awareness must take place, advising employees on a need-to-know basis on how SPI is processed.

28 - AUTHORISATION CONCERNING DATA SUBJECT’S RELIGIOUS OR PHILOSOPHICAL BELIEFS

The prohibition on processing Personal Information concerning a Data Subject’s **religious or philosophical** beliefs, **does not apply if** the processing is carried out by—

- (a) spiritual or religious organisations, or independent sections of those organisations if—
 - (i) the information concerns Data Subjects belonging to those organisations; or (ii) it is necessary to achieve their aims and principles;
- (b) institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or
- (c) other institutions: Provided that the processing is necessary to protect the spiritual welfare of the Data Subjects, unless they have indicated that they object to the processing.

In the cases referred to above, the prohibition does not apply to processing of Personal Information concerning the religion or philosophy of life of family members of the Data Subjects, if—

- (a) the association concerned maintains regular contact with those family members in connection with its aims; and
- (b) the family members have not objected in writing to the processing.

In the cases referred to above, Personal Information concerning a Data Subject’s religious or philosophical beliefs may not be supplied to third parties without the consent of the Data Subject.

1. The Responsible Party may only process **religious or philosophical** beliefs which it may require for a number of reasons, such as the treatment of the employee or student on the campus or workplace **with the consent of the Data Subject** as the justifications will not apply to it.
2. However, where the Responsible Party processes a Data Subject’s **religious or philosophical** beliefs in order to protect the spiritual welfare of the Data Subject, it can without the required consent unless the person has indicated that they object to the processing.
3. Ensure such processing of **religious or philosophical** for the protection of the spiritual welfare of the Data Subject’s included under the Section 18 Notice.
4. The Responsible Party must take note of the other justifications and conditions are as follows:
 - Churches may process a member’s **religious or philosophical** beliefs, **but** a Data Subject’s religious or philosophical beliefs may not be supplied to third parties without the consent of the Data Subject.
5. Ensure that training and awareness sessions are conducted on the requirements pertaining to the processing of **religious or philosophical** beliefs.



29 - AUTHORISATION CONCERNING DATA SUBJECT'S RACE OR ETHNIC ORIGIN

The prohibition on processing Personal Information concerning a Data Subject's race or ethnic origin, **does not apply if** the processing is carried out to identify Data Subjects and only when this is essential for that purpose and comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

1. The Responsible Party may only process a Data Subject's race or ethnic origin if the processing is carried out to identify Data Subjects and only when this is essential for that purpose and to comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination. **This processing should be done in line with B-BBEE laws.**
2. Ensure that Training and awareness sessions are conducted on the requirements pertaining to the processing of **a Data Subject's race or ethnic origin.**

30 - AUTHORISATION CONCERNING DATA SUBJECT'S TRADE UNION MEMBERSHIP

The prohibition on processing Personal Information concerning a Data Subject's trade union membership, does not apply to the processing by the trade union to which the Data Subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union or trade union federation.

In the cases referred to above, no Personal Information may be supplied to third parties without the consent of the Data Subject.

1. The Responsible Party may only process a Data Subject's trade union membership with the Data Subjects permission and consent and for the purposes of processing of union membership deductions
2. Consent should be detailed under the section 18 processing document and housed in the form of a stop order deduction form authorised by the employee.
3. Ensure that training and awareness sessions are conducted on the requirements pertaining to the processing of **a Data Subject's trade union membership.**



31 - AUTHORISATION CONCERNING DATA SUBJECT'S POLITICAL PERSUASION

The prohibition on processing Personal Information concerning a Data Subject's political persuasion, does not apply to processing by or for an institution, founded on political principles, of the Personal Information of—

- (a) its members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution; or
- (b) a Data Subject if such processing is necessary for the purposes of—
 - (i) forming a political party;
 - (ii) participating in the activities of, or engaging in the recruitment of members for or canvassing supporters or voters for, a political party with the view to—
 - (aa) an election of the National Assembly or the provincial legislature as regulated in terms of the Electoral Act, 1998 (Act No. 73 of 1998);
 - (bb) municipal elections as regulated in terms of the Local Government: Municipal Electoral Act, 2000 (Act No. 27 of 2000); or
 - (cc) a referendum as regulated in terms of the Referendums Act, 1983 (Act No. 108 of 1983); or
 - (iii) campaigning for a political party or cause.

In the cases referred to above no Personal Information may be supplied to third parties without the consent of the Data Subject.

The processing of Personal Information concerning a Data Subject's political persuasion is prohibited.

Following this, don't ask anyone about their political persuasions.

32 - AUTHORISATION CONCERNING DATA SUBJECT'S HEALTH OR SEX LIFE

The prohibition on processing Personal Information concerning a Data Subject's health or sex life, does not apply to the processing by—

- (a) medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the Data Subject, or for the administration of the institution or professional practice concerned;
- (b) insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for—
 - (i) assessing the risk to be insured by the insurance the Responsible Party or covered by the medical scheme and the Data Subject has not objected to the processing;
 - (ii) the performance of an insurance or medical scheme agreement; or
 - (iii) the enforcement of any contractual rights and obligations;
- (c) schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;
- (d) any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;
- (e) any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or
- (f) administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for—
 - (i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the Data Subject; or
 - (ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

The Responsible Party must ensure that all Special Personal Information concerning a Data Subject's health or sex life, is only processed with the consent of the Data Subject or where it can show that there was a legitimate reason or requirement for the processing of such information or such processing is subject to an allowed exception, or in terms of applicable legislation.

The Responsible Party must educate all its employees about this section 32 - making them all aware of the fact that one may not process Personal Information concerning a Data Subject's health or sex life, unless the processing is:

- (a) conducted by a Responsible Party appointed medical professional, healthcare institution or facility and such processing is necessary for the proper treatment and care of the Data Subject, or for the administration of the institution or professional practice concerned;
- (b) conducted by a Responsible Party appointed insurance company, medical scheme, medical scheme administrator and/or managed healthcare organisation, if such processing is necessary for—
 - (i) assessing the risk to be insured by the insurance company or covered by the medical scheme and the Data Subject has not objected to the processing;
 - (ii) the performance of an insurance or medical scheme agreement; or
 - (iii) the enforcement of any contractual rights and obligations.
- (f) conducted by a Responsible Party appointed administrative body, pension fund, employer or institution working for it, if such processing is necessary for—
 - (i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the Data Subject; or
 - (ii) the reintegration of, or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

When a third party processes the above information, the Responsible Party must obtain undertakings of confidentiality under a written agreement from the person who is processing the information, prior to the processing.



<p>In the cases referred to above, the information may only be processed by responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the Responsible Party and the Data Subject.</p>	<p>Ensure that training and awareness sessions are conducted on the requirements pertaining to the processing of a Data Subject’s health or sex life.</p>
---	---

<p>33 - AUTHORISATION CONCERNING DATA SUBJECT’S CRIMINAL BEHAVIOUR OR BIOMETRIC INFORMATION</p> <p>The prohibition on processing Personal Information concerning a Data Subject’s criminal behaviour or biometric information, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law.</p> <p>The processing of information concerning personnel in the service of the Responsible Party must take place in accordance with the rules established in compliance with labour legislation.</p> <p>The prohibition on processing any of the categories of Personal Information referred to in POPIA does not apply if such processing is necessary to supplement the processing of information on criminal behaviour or biometric information permitted by this section.</p>	<p>The Responsible Party must ensure that all special person information concerning a Data Subject’s criminal behaviour or biometric information, is only processed with the consent of the Data Subject, or where it can show that the processing of information concerning personnel in the service of the Responsible Party concerning criminal or deviant behaviour has been or will be done in accordance with the rules established in compliance with labour legislation.</p> <p>Following this, ensure that all background check forms which give the Responsible Party permission to do biometric processing or criminal checks, verification of education and employment and financial standing are signed by the Data Subjects before their information is collected.</p> <p>Ensure that this consent and detail on processing is inserted in the section 18 processing form or notice.</p>
---	--

34 - PROHIBITION ON PROCESSING PERSONAL INFORMATION OF CHILDREN

A Responsible Party may, subject to POPIA, not process Personal Information concerning a child.

35-GENERAL AUTHORISATION CONCERNING PERSONAL INFORMATION OF CHILDREN

The prohibition on processing Personal Information of children, as referred to above, does not apply if the processing 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 in law;
- (c) necessary to comply with an obligation of international public law;
- (d) for historical, statistical or research purposes to the extent that—
 - (i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or
 - (ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- (e) of Personal Information which has deliberately been made public by the child with the consent of a competent person.

The Regulator may, subject to the below, upon application by a Responsible Party and by notice in the Gazette, authorise a Responsible Party to process the Personal Information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the Personal Information of the child. The Regulator may impose reasonable conditions in respect of any authorisation granted as set out above including conditions with regard to how a Responsible Party must—

1. The Responsible Party must have procedures in place which govern the processing of children’s Personal Information so as to ensure that it is only processed with the prior consent of a competent person; or is processed because it is necessary for the establishment, exercise or defence of a right or obligation in law; or necessary to comply with an obligation of international public law; or is for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or of Personal Information which has deliberately been made public by the child with the consent of a competent person.
2. The parent or legal guardian must sign all documents which house Personal Information of children.
3. Training and awareness on the requirements must be carried out and this requirement must form part of the training material.

- (a) upon request of a competent person provide a reasonable means for that person to—
 - (i) review the Personal Information processed; and
 - (ii) refuse to permit its further processing;
- (b) provide notice—
 - (i) regarding the nature of the Personal Information of children that is processed;
 - (ii) how such information is processed; and
 - (iii) regarding any further processing practices;
- (c) refrain from any action that is intended to encourage or persuade a child to disclose more Personal Information about him- or herself than is reasonably necessary given the purpose for which it is intended; and
- (d) establish and maintain reasonable procedures to protect the integrity and confidentiality of the Personal Information collected from children.



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
13 RIGHT TO CORRECT PERSONAL INFORMATION		
<p>Can a Data Subject ask for its Personal Information to be updated?</p> <p>How must this be done?</p> <p>How must the Responsible Party react when it receives a request to update details?</p>	<p>A Data Subject may, using the prescribed form set out under the regulations, request a Responsible Party to—</p> <p>(a) correct or delete Personal Information about the Data Subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or</p> <p>(b) destroy or delete a record of Personal Information about the Data Subject that the Responsible Party is no longer authorised to retain in terms of POPIA.</p> <p>On receipt of a request in terms of the above a Responsible Party must, as soon as reasonably practicable—</p> <p>(a) correct the information;</p> <p>(b) destroy or delete the information;</p> <p>(c) provide the Data Subject, to his or her satisfaction, with credible evidence in support of the information; or</p> <p>(d) where agreement cannot be reached between the Responsible Party and the Data Subject, and if the Data Subject so requests, take such steps as are reasonable in the 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.</p>	<p>The Responsible Party must ensure that all Data Subjects are made aware of their right to request that the Responsible Party amends or rectifies their Personal Information, by implementing the following controls:</p> <ol style="list-style-type: none"> 1. Annual Update of Information Form circulated / distributed requesting Data Subjects to validate and sign-off on the correctness of their Personal Information in the possession of the Responsible Party. 2. Annual Supplier and other Third Party held Data Forms containing third party's Personal Information, is distributed requesting Data Subjects to validate and sign-off on the correctness of their Personal Information in the Responsible Party's possession. 3. Annual Student held Data Forms containing student Personal Information, is distributed requesting Data Subjects to validate and sign-off on the correctness of their Personal Information in the Responsible Party's possession. 4. Ensure that the Data Subjects are aware of their right to request for amendments or deletion of the Personal Information under standard section 18 form with hyperlink to update form. 5. Training and awareness sessions on the requirements to update Personal Information provided to all staff. 6. Upon receipt of the annual form that contains the Data Subject's personal Data, the information is updated timeously on the Responsible Party's systems. 7. Where employees request for additions and deletions of Personal Information, they produce proof / supporting documents, i.e. ID, birth certificates, marriage certificate, etc. - this information is then captured on the system and stored in the employee's personnel and e-filing system.

		<p>8. Ensure that the lawful requests of the Data Subject are acceded to.</p> <p>9. Development of the SOP document to include to the requirements herein.</p> <p>10. Employees complete forms that are sent to pension fund, or Medical Aid, etc., informing them of their Data amendments.</p> <p>11. Procedures in place to ensure that on receipt of a request from a Data Subject to correct or amend Personal Details, that as soon as reasonably practicable the Responsible Party corrects the information; destroys or delete the information; provides the Data Subject, to his or her satisfaction, with credible evidence in support of the information; or where agreement cannot be reached between the Responsible Party and the Data Subject, and if the Data Subject so requests, the Responsible Party must take such steps as are reasonable in the 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.</p> <p>If the Responsible Party has taken steps as set out above 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, the Responsible Party must, if reasonably practicable, inform each person or body or Responsible Party to whom the Personal Information has been disclosed of those steps.</p> <p>The Responsible Party must notify a Data Subject, who has made a request in terms of the above, of the action taken as a result of the request.</p> <p>SEE STANDARD RESPONSIBLE PARTY UPDATE OF INFORMATION FORM AND SEND OUT REGULAR UPDATE TO INFORMATION REQUEST</p>
--	--	---



QUESTION	ANSWER	ACTION, REFERENCE TO ACT AND PROCESSING DOCUMENTS
14 INFORMATION OFFICERS	<p>Who is an Information Officer?</p> <p>An Information Officer is a person, as described under PAIA, who is <i>the head of an entity</i>. This person may delegate this duty in a public entity to another, provided this is in writing.</p> <p>In the private sphere the CEO may appoint an Information Officer to act as such under a formal appointment.</p> <p>This function in the main will ensure that the POPIA and PAIA laws are implemented within the operation and complied with.</p> <p>In terms of POPIA, an Information Officer's responsibilities include ensuring:</p> <ul style="list-style-type: none"> • compliance by the body with the conditions for the lawful processing of Personal Information; • dealing with requests made to the body pursuant to this Act; • working with the Regulator in relation to investigations • that a compliance framework is developed, implemented and monitored; • that adequate measures and standards exists to comply with the conditions for the lawful processing of Personal Information; • that preliminary assessments are conducted; • that a manual for the purpose of the Promotion of Access to Information Act and the Act is developed detailing - the purpose of the processing; a description of the categories of Data Subjects and of the information or categories of information relating thereto; the recipients or categories of recipients to whom the Personal Information may be supplied; 	<p>SECTION 55 - DUTIES AND RESPONSIBILITIES OF INFORMATION OFFICER</p> <p>SECTION 56 - DESIGNATION AND DELEGATION OF DEPUTY INFORMATION OFFICERS</p> <ol style="list-style-type: none"> 1. The Responsible Party must appoint an Information Officer who understands his or her role, responsibilities and duties. 2. The Information Officer must be registered with the Regulator. 3. The Responsible Party needs to appoint Information Officers before the legislation comes in effect. This appointment should be done with due consideration of PAIA. 4. Appoint a Deputy Information Officer where necessary 5. Roles and responsibilities of the Information Officers / Deputies must be developed and clarified. 6. A process needs to be developed and implemented on how an Information Officer will be supported to carry out his or her responsibilities, including dealing with the information Regulator. 7. Information Officer to undergo training and awareness on the 8 conditions of POPIA in terms of lawful processing of Personal Information <p>SEE REGISTRATION OF IO AND DIO</p> <p>SEE DETAILS IN PAIA MANUAL</p>

	<p>the planned trans-border or cross border flows of Personal Information; and a general description allowing preliminary assessment of the suitability of information security measures to be implemented and monitored by the Responsible Party;</p> <ul style="list-style-type: none"> • that the manual is available on the website of the Responsible Party; and at the office or offices of the Responsible Party for public inspection during normal business hours of that Responsible Party; • that internal measures are developed together with adequate systems to process requests for information or access thereto; and • that 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. <p>Officers must take up their duties in terms of this Act only after the Responsible Party has registered them with the Regulator.</p> <p>Furthermore, each public and private body must make provision for the designation of such a number of persons, if any, as deputy Information Officers as is necessary to perform the duties and responsibilities as set out this Act; and any power or duty conferred or imposed on an Information Officer by this Act to a Deputy Information Officer of that public or private body.</p>	
--	---	--