
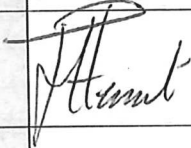
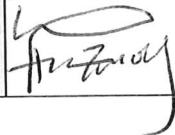


# GOLD ONE

## GROUP LIMITED

Reference No.	11.06.2021	Effective Date	1 JULY 2021
---------------	------------	----------------	-------------

### PERSONAL INFORMATION SHARING POLICY

Compiled by	Legal Advisor	Signature		Date	22-07-21
Reviewed	Mancom	Signature		Date	27/07/2021
Approved	Exco	Signature		Date	27/07-2021

1. **PURPOSE**

The purpose of this policy is to deal with:

- 1.1. internal and external requests for the sharing of Personal Information;
- 1.2. controls needed for information sharing; and
- 1.3. the expected standards when Personal Information is shared.

2. **DEFINITIONS**

Unless otherwise determined by the context, the words and expressions used in this policy shall bear the meaning assigned to them below:

- 2.1. "Authorised Third Parties" all third parties who Process the Personal Information of Gold One's Data Subjects on behalf of Gold One or as part of any functions or duties which they carry out (whether contractual or otherwise) for Gold One;
- 2.2. "Data Subject" means a person to whom Personal Information relates;
- 2.3. "Deputy Information Officer" means the person designated as such by the Information Officer in terms of section 56 of POPIA and/or section 17 of the Promotion of Access to Information Act, 2 of 2000;
- 2.4. "Further Processing" refers to the Processing of Personal Information for a purpose other than that for which it was initially collected.
- 2.5. "Information Officer" means the person appointed as Gold One's chief executive officer, or equivalent officer, or the person who is acting as such, or the person authorised by such officer;
- 2.6. "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:
  - 2.6.1. 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;
  - 2.6.2. information relating to the education or the medical, financial, criminal or employment history of the person;
  - 2.6.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

- 2.6.4. the biometric information of the person;
- 2.6.5. the personal opinions, views or preferences of the person;
- 2.6.6. 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;
- 2.6.7. the views or opinions of another individual about the person; and
- 2.6.8. 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;
- 2.7. "POPIA" means the Protection of Personal Information Act 13 of 2013, and any regulations published under that legislation;
- 2.8. "Employees" means all employees, directors, officers, agency workers and other staff of Gold One;
- 2.9. "Public Authority" means any governmental or regulatory body established in terms of relevant legislation;
- 2.10. "Processing" or "Process" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including:
- 2.10.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- 2.10.2. dissemination by means of transmission, distribution or making available in any other form; or
- 2.10.3. merging, linking, as well as restriction, degradation, erasure or destruction of information;
- 2.11. "Special Personal Information" means Personal Information relating to: (i) 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 (ii) the criminal behaviour of a Data Subject to the extent that such intimation relates to: (a) the alleged commission by a data Subject of any offence; or (b) any proceedings in respect of an offence allegedly committed by a Data Subject or the disposal of such proceeding; and
- 2.12. "Unconnected Third Party" means a third party which is not a customer, vendor, business partner, or operator of Gold One.

### 3. APPLICATION OF THIS POLICY

This policy applies to all Employees who are subject to the conditions and scope of this policy.

### 4. OBLIGATIONS

#### 4.1. Purpose, definition and limitation

4.1.1. Personal Information may only be collected and Further Processed for lawful, specific and explicitly defined purposes related to a function or activity of Gold One.

4.1.2. After Personal Information has been collected by Gold One, it may not be Processed for purposes which are incompatible with the original purpose. For example, this means that Personal Information Processed by the human resources team for HR purposes may not be lawfully Processed by the marketing team for marketing purposes.

4.1.3. Where a Data Subject wishes to access his, her or its own Personal Information, the Data Subject Access Request Policy should be adhered to.

#### 4.2. Personal information to be kept confidential

Gold One must keep Personal Information confidential and safe from undue disclosures. That means that sharing Personal Information with third parties is an exception to the confidentiality rule, and must be analysed in detail to ensure lawfulness, notably by considering:

4.2.1. whether the purpose for which the third party requires the Personal Information is compatible to the original purpose for which the information was collected;

4.2.2. whether sharing the Personal Information with the third party will constitute a transborder flow of information; and

4.2.3. whether sharing the Personal Information with the third party will likely put the information at risk due to the poor security measures the third party has in place.

### 5. PROCEDURES TO FOLLOW

5.1. Employees that receive a request for Personal Information must notify the Information Officer or the Deputy Information Officer who will provide guidance or, as the case may be, lead the procedures.

5.2. Employees that are required to share Personal Information, must consider whether the Personal Information is to be shared internally (i.e., within Gold One) or externally (i.e., with an Authorised Third Party, a Public Authority or an Unconnected Third Party).

- 5.3. Employees that are unsure which category the Personal Information sharing falls into must contact the Information Officer or the Deputy Information Officer for further guidance.
- 5.4. Employees must document at all times any questions asked, responses received, and authorisation gained by any parties involved when dealing with a Personal Information sharing request.
- 5.5. The Information Officer and Deputy Information Officer will Process all requests for Personal Information by Unconnected Third Parties and Public Authorities.

## 6. PERSONAL INFORMATION SHARING

- 6.1. Personal Information may be shared internally between divisions for the day-to-day business operations of Gold One and on a need-to-know basis.
- 6.2. Personal Information may also be shared internally to carry out duties in terms of contracts, legislation and subordinate legislation and the like.
- 6.3. There should be a clear objective or set of objectives for sharing Personal Information with Authorised Third Parties. Being clear about this will identify the following:
  - 6.3.1. Could the objective be achieved without sharing the information or by de-identifying (anonymising) it?
  - 6.3.2. What information needs to be shared? Employees should not share all the Personal Information they hold about a Data Subject if only certain items are needed to achieve the objectives.
  - 6.3.3. Who requires access to the shared Personal Information? Employees should employ 'need to know' principles, third parties should only have access to Personal Information if they need it to do their job, and that only relevant staff should have access to the information. This should also address any necessary restrictions on onward sharing of information with third parties.
  - 6.3.4. When should it be shared? It is good practice to document this and set out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.
  - 6.3.5. How should it be shared? This involves addressing the security surrounding the transmission or accessing of the information and establishing common rules for its security.
  - 6.3.6. How can we check the sharing is achieving its objectives? Employees will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.

- 6.3.7. How are Data Subjects made aware of the information sharing? Has the sharing been addressed in Gold One's external or internal privacy policy?
- 6.3.8. What risk to the Data Subjects and/or the organisation does the information sharing pose? For example, is any Data Subject likely to be damaged by it? Is any Data Subject likely to object? Might it undermine a Data Subject's trust in Gold One?
- 6.3.9. What is the legal basis for Processing the information? Employees must identify the lawful basis (e.g., meeting statutory duties) for Processing and, where necessary, a condition for Processing Special Personal Information (e.g., consent).
- 6.3.10. If the information is confidential, what is the legal basis that complies with the common law duty of confidence? This can be consent (implied or explicit), overriding public interest or required or permitted by law.
- 6.4. Personal Information should not be shared with Unconnected Third Parties or Public Authorities, without seeking further guidance from the Information Officer or the Deputy Information Officer.
- 6.5. It is good practice to document all decisions and reasoning related to the information sharing.

## 7. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all Employees comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for Gold One and its Employees. Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

## 8. POLICY REVISION

The Information Officer will be responsible for reviewing this policy at regular intervals, when appropriate, to ensure that it meets legal requirements and reflects best practice.

